#6

Docket No.: 50023-161 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

jc781 U.S. PTO 10/023483 12/20/01

In re Application of	:	
Hiroki YAMAUCHI, et al.	:	
Serial No.:	:	Group Art Unit:
Filed: December 20, 2001	:	Examiner:

For: DATABASE MANAGEMENT DEVICE, DATABASE MANAGEMENT METHOD AND STORAGE MEDIUM THEREFOR

CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Commissioner for Patents
Washington, DC 20231

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2000-392661, filed December 25, 2000

A Certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Stephen A. Becker
Registration No. 26,527

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 SAB:prp
Date: December 20, 2001
Facsimile: (202) 756-8087

50023-161
H. YAMAUCHI et al.
Dec. 20, 2001

日　本　国　特　許　庁
JAPAN PATENT OFFICE

McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１２月２５日

出願番号
Application Number: 特願２０００－３９２６６１

出願人
Applicant(s): 松下電器産業株式会社

２００１年　９月１３日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０８４７５０

【書類名】　特許願
【整理番号】　2022520458
【提出日】　平成12年12月25日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 17/30
G06F 12/547
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　山内　弘貴
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　山口　雅史
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100083172
【弁理士】
【氏名又は名称】　福井　豊明
【手数料の表示】
【予納台帳番号】　009483
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9713946

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　データベース管理装置、管理方法及びその記録媒体

【特許請求の範囲】

【請求項１】　有効期間を含む必要事項より構成される情報を一データ単位とし、当該データの有効期間が終了するに際して該データに対応する後継データを作成するデータベース管理装置において、

有効期間が終了する所定のデータと、当該所定のデータに対応する後継データとの両方又はいずれか一方に上記データを相互に関連付けた関連情報を追加する関連情報追加手段を具備することを特徴とするデータベース管理装置。

【請求項２】　さらに、上記所定のデータ又は上記後継データの参照時に、当該データに含まれる上記関連情報を参照して対応するデータを検索する関連情報検索手段を具備する請求項１に記載のデータベース管理装置。

【請求項３】　上記データは、ＩＰＳＥＣ(Internet Protocol Security Protocol) 通信に用いられるＳＡ（Security Association）である請求項２に記載のデータベース管理装置。

【請求項４】　有効期間を含む必要事項より構成される情報を一データ単位とし、当該データの有効期間が終了するに際して該データに対応する後継データを作成するデータベース管理装置において、

上記有効期間と、当該有効期間を含むデータの参照情報とを関連付けて記憶すると共に、当該有効期間の終了に際してその旨を通知する有効期間管理手段と、

有効期間管理手段からの通知を受けて、上記データに対して当該有効期間終了に伴う所定の処理を行うデータ制御手段とを備えることを特徴とするデータベース管理装置。

【請求項５】　上記所定の処理が、上記対応する後継データの作成である請求項４に記載のデータベース管理装置。

【請求項６】　上記所定の処理が、上記有効期間が終了するデータの削除である請求項４に記載のデータベース管理装置。

【請求項７】　上記必要事項より構成される情報が、上記有効期間が終了する前に上記後継データを作成すべき時間情報を含むデータベース管理装置において

更に、上記時間情報と、当該時間情報を含むデータの参照情報とを関連付けて記憶すると共に、当該時間情報にて示された時間の到来を通知する更新管理手段と、

上記更新管理手段からの通知を受けて、上記後継データを作成する上記データ制御手段とを備える請求項４に記載のデータベース管理装置。

【請求項８】　上記有効期間が終了する所定のデータと、当該所定のデータに対応する後継データとの両方又はどちらか一方に上記データを相互に関連付けた関連情報を追加する関連情報追加手段を具備する請求項４又は７に記載のデータベース管理装置。

【請求項９】　上記有効期間の終了を延長する延長期間情報を記憶すると共に、上記有効期間が終了するに際して、当該有効期間が終了するデータの有効期間を上記延長期間情報が示す期間延長する有効期間延長手段を具備する請求項８に記載のデータベース管理装置。

【請求項１０】　上記後継データの作成時に、当該後継データの検索順序を、該後継データに対応するデータの前方に位置させる検索順序管理手段を備える請求項４又は７に記載のデータベース管理装置。

【請求項１１】　さらに、上記後継データと該後継データに対応するデータの検索頻度を監視する検索頻度監視手段を備え、

上記検索順序管理手段は、上記検索頻度に基づいて上記所定のデータと上記後継データの検索順序を変更する請求項４又は７に記載のデータベース管理装置。

【請求項１２】　上記データは、ＩＰＳＥＣ(Internet Protocol Security Protocol) 通信に用いられるＳＡ (Security Association) である請求項４に記載のデータベース管理装置。

【請求項１３】　有効期間を含む必要事項より構成される情報を一データ単位とし、当該データの有効期間が終了するに際して該データに対応する後継データを作成するデータベース管理方法において、

有効期間が終了する所定のデータと、当該所定のデータに対応する後継データとの両方又はいずれか一方に上記データを相互に関連付けた関連情報を追加する

ステップと

上記所定のデータ又は上記後継データの参照時に、当該データに含まれる上記関連情報を参照して対応するデータを検索するステップとを具備することを特徴とするデータベース管理方法。

【請求項１４】　有効期間を含む必要事項より構成される情報を一データ単位とし、当該データの有効期間が終了するに際して該データに対応する後継データを作成するデータベース管理方法において、

上記有効期間と、当該有効期間を含むデータの参照情報とを関連付けて記憶すると共に、当該有効期間の終了に際してその旨を通知するステップと、

有効期間管理手段からの通知を受けて、上記データに対して当該有効期間終了に伴う所定の処理を行うステップとを備えることを特徴とするデータベース管理方法。

【請求項１５】　有効期間を含む必要事項より構成される情報を一データ単位とし、当該データの有効期間が終了するに際して該データに対応する後継データをコンピュータにより作成するステップを記録した記録媒体において、

有効期間が終了する所定のデータと、当該所定のデータに対応する後継データとの両方又はどちらか一方に上記データを相互に関連付けた関連情報を追加するステップと

上記所定のデータ又は上記後継データの参照時に、当該データに含まれる上記関連情報を参照して対応するデータを検索するステップとを記録したことを特徴とするコンピュータ読取可能な記録媒体。

【請求項１６】　有効期間を含む必要事項より構成される情報を一データ単位とし、当該データの有効期間が終了するに際して該データに対応する後継データをコンピュータにより作成するステップを記録した記録媒体において、

上記有効期間と、当該有効期間を含むデータの参照情報とを関連付けて記憶すると共に、当該有効期間の終了に際してその旨を通知するステップと、

有効期間管理手段からの通知を受けて、上記データに対して当該有効期間終了に伴う所定の処理を行うステップとを記録したことを特徴とするコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データベース管理装置、管理方法及びその記録媒体に係り、詳しくは、データが有効期間を持つデータベースのデータベース管理装置、管理方法及びその記録媒体に関するものである。

【０００２】

【従来の技術】

近年、ＴＣＰ／ＩＰプロトコルを用いたインターネットは、研究教育用ネットワークとしての役割のみならず、インターネットあるいは企業間のイントラネットを介した電子メールの交換や、これらを利用した電子商取引や電子決済にも利用されており、社会と個人のコミュニケーション用ネットワークとしての役割を担う情報通信基盤となっている。

【０００３】

しかし、元来インターネットには通信中の情報の秘匿化や改ざんを防止する機能がないため、容易に通信中の情報を盗聴、改ざんすることができた。従って、特に重要な情報を含む通信には専用線並のセキュリティの確保が重要である。

【０００４】

上述したようなセキュリティを確保する技術として、例えばインターネットのような広域ネットワークを仮想私設網とするＶＰＮ(Virtual Private Network)技術等のセキュリティ通信技術が注目されている。ＶＰＮを実現するセキュリティ通信のための接続手順としてトンネリングプロトコルがあり、Ｌ２Ｆ(Layer 2 Forwarding)、ＰＰＴＰ(Point-to-Point Tunneling Protocol)、Ｌ２ＴＰ(Layer 2 Tunneling Protocol)、ＡＴＭＰ(Ascend Tunnel Management Protocol)、ＢａｙＤＶＳ(BayStream Dial VPN Service)、ＩＰＳＥＣ(Internet Protocol Security Protocol)等が標準化されている。上記セキュリティ通信のためのプロトコルを使用することにより、第３者が通信を盗聴しうる上記広域ネットワークにおいて通信のセキュリティを確保することが可能となる。

【０００５】

このようなセキュリティ通信技術のうち、上記ＩＰＳＥＣは、ネットワーク層（ＯＳＩ参照モデル(Open System Interconnection reference model) 第３層）で認証、暗号化を行うセキュリティプロトコルであり、インターネット技術の標準化機構であるＩＥＴＦ（Internet Engineering Task Force ）によって標準化されている。その標準化の過程としては、１９９５年８月にＩＰプロトコルにさまざまセキュリティ機能を付加したＩＰＳＥＣプロトコルバージョン１が標準化され、さらに１９９８年１１月にはＩＰＳＥＣプロトコルバージョン１に改訂や機能の拡張を施したＩＰＳＥＣプロトコルバージョン２と暗号認証鍵交換用ＩＫＥプロトコルが標準化された。

【０００６】

上記ＩＰＳＥＣ機能を搭載したコンピュータや、ネットワーク接続装置であるルータ等を介してインターネットに接続することにより、上記ＶＰＮを構築することが可能である。即ち、ユーザはネットワークの種類を意識することなく、安全にインターネットを利用することができる。尚、ＩＰＳＥＣを利用した通信を行うにあたっては、どのような認証アルゴリズムや暗号化アルゴリズムを使用するか、あるいはどのような暗号化鍵を使用するかなどを、事前に送信側と受信側のＩＰＳＥＣ機能を搭載したコンピュータ、または、ネットワーク接続装置間で整合を取っておく必要がある。この認証、暗号化アルゴリズムの整合をとるための相互通信を、セキュリティ通信のための接続と呼ぶ。

【０００７】

ＩＰＳＥＣにおいては、この接続はＳＡ（Security Association）によって実現されている。上記ＳＡは認証とセキュアメッセージ交換の機能を提供する基本的な枠組であり、その通信のセキュリティのいくつかの側面を定義する。

【０００８】

以下に、図９、図１０、図１１、図１２を参照しながら、従来の、セキュリティ通信としてＩＰＳＥＣを用いた通信方法について説明する。又、ここに通信端末とは、ネットワーク接続装置及びコンピュータを含む。

【０００９】

図９は、従来のセキュリティ通信としてＩＰＳＥＣ機能を搭載したルータを使

用してＶＰＮネットワークを構成したネットワークシステムの概略図、図１０は、上記ＩＰＳＥＣ機能を搭載したネットワーク接続装置間でのセキュリティ通信の接続手順を表した図、図１１は、従来技術におけるＩＰＳＥＣの処理方針を決めるデータベースであるＳＰＤ（Security Policy Database）の例、図１２は、従来技術におけるＳＡデータベースであるＳＡＤ（Security Association Database)の例である。ここに、ＳＰＤとはセキュリティポリシーを構成するデータベースである。又、セキュリティポリシーとは、セキュリティを確保されたシステムへのアクセス規制のことであり、一般にセキュリティ要件、セキュリティ上のリスク、及びセキュリティの測定手段が含まれる。通信端末間のセキュリティを確保するシステムにおいては、セキュリティを適用する相手先通信端末を区別する情報、セキュリティを適用するかどうかの情報等を備える。尚、ＩＰＳＥＣにおいては、セキュリティポリシーは上記ＳＰＤに記述され、該ＳＰＤには送信先通信端末のＩＰアドレス、ＩＰＳＥＣ処理の有無、認証、暗号化アルゴリズム等の内容を記述した上記ＳＡが格納されるメモリ上のアドレスの参照情報を備える。

【００１０】

図９において、コンピュータ９０１はＬＡＮ９０７(Local Area Network)で他のコンピュータ９０５及びネットワーク接続装置９０２と接続されており、ネットワーク接続装置９０２を経由して、外部のインターネット９０９やイントラネット等のＷＡＮに接続されている。このインターネット９０９には他のネットワーク接続装置９０３を介してコンピュータ９０４、９０６が接続されるＬＡＮ９０８が接続されている。ここで、上記ネットワーク接続装置９０２、９０３は、ルータ、ゲートウエイ、プロキシサーバ等のファイアウォールやＶＰＮ専用装置等である。尚、コンピュータ９０１他は、パーソナルコンピュータ、ワークステーション、サーバ、ノート型パソコン、ＩＰ電話、ＩＰテレビ電話、ＩＰ携帯電話等の通信機能をもつ端末であればよい。

【００１１】

ここでは上記ネットワーク接続装置９０２、９０３にＩＰＳＥＣ機能を搭載し、ネットワーク接続装置９０２、９０３間でＩＰＳＥＣによる通信を行うものと

して説明する。また、上記コンピュータ９０１及び９０４にＩＰＳＥＣ機能を搭載し、上記コンピュータ９０１、９０４間でＩＰＳＥＣによる通信を行うことも可能である。さらに、同様にＩＰＳＥＣ機能を搭載した、コンピュータ９０１とＩＰＳＥＣ機能を搭載しているネットワーク接続装置９０３間でＩＰＳＥＣによる通信を行うことも可能である。

【００１２】

さて、コンピュータ９０１がインターネット９０９を介してコンピュータ９０４にデータを送信する場合には、予め上記ネットワーク接続装置９０２、９０３間において上記セキュリティ通信のための接続を行う必要がある。以下に該セキュリティ通信のための接続について説明する。

【００１３】

ＩＰＳＥＣ通信を始めるにあたり、まず、ＩＰＳＥＣの暗号鍵交換のためのプロトコルであるＩＫＥ（Internet Key Exchange)が用いられる。該ＩＫＥを使用した通信は、ＩＫＥフェーズ１とＩＫＥフェーズ２とに分けて説明することができ、上記ネットワーク接続装置９０２、９０３間で行われる。尚、ＩＫＥによる自動鍵交換を行わず、手動で秘密鍵の交換を行ってもよい。

【００１４】

上記ＩＫＥフェーズ１（図１０：Ｓ１００１）では、ＩＫＥ自身が安全に通信を行うために、互いに利用可能なＳＡ(Security Association)を確立するための情報を交換する。ここでＳＡとは、例えば、認証アルゴリズムや認証パラメータ、暗号化アルゴリズムや暗号化パラメータ等を含む一連の定義情報群である。

【００１５】

次に、ＩＫＥフェーズ２（図１０：Ｓ１００２）では、前記ＩＫＥフェーズ１にて確立した上記ＳＡを用いて、ＩＰＳＥＣ通信用のＳＡに関する情報を交換する。ここで、ＩＰＳＥＣ通信用のＳＡの一例について図１２に示す。図１２は、複数の上記ＳＡである、ＳＡ１（１２０２）～ＳＡＭ（１２０４）を含むＳＡＤ１２０１であり、さらに各ＳＡには送信ホストアドレス１２０５、受信ホストアドレス１２０６、プロトコル１２０７、当該ＳＡのインデックス情報であるＳＰＩ１２０８（Security Parameters Index）、登録時刻１２０９、有効期間１２

１０、更新待ち期間１２１１、認証アルゴリズム１２１２、認証鍵１２１３、暗号化アルゴリズム１２１４、暗号化鍵１２１５等が含まれる。

【００１６】

上記送信ホストアドレス１２０５には送信元ＩＰアドレス、送信元ポート番号が、上記受信ホストアドレス１２０６には送信先ＩＰアドレス、送信先ポート番号が、プロトコル１２０７にはプロトコル番号等が含まれる。又、上記ＳＰＩ１２０８には擬似乱数等が用いられ、当該ＳＡを特定可能となっている。

【００１７】

さらに、登録時刻１２０９には当該ＳＡを登録した時刻が、有効期間１２１０には当該ＳＡの有効期間が、更新待ち期間１２１１には当該ＳＡの更新迄の期間がそれぞれ格納されているが詳細は後述する。

【００１８】

さらに、認証アルゴリズム１２１２には例えばＨＭＡＣ－ＭＤ５－９６といった認証アルゴリズムが、暗号化アルゴリズム１２１４には例えばＤＥＳ－ＣＢＣといった暗号化アルゴリズムの種別が格納され、認証鍵１２１３及び暗号化鍵１２１５はそれぞれの認証、暗号化（復号化）に必要な鍵が格納される。

【００１９】

上記ＩＫＥフェーズ２（１００２）で行われるＩＰＳＥＣ通信用のＳＡに関する情報の交換は、具体的には、ネットワーク接続装置９０２がネットワーク接続装置９０３に対し、ＩＰＳＥＣ通信に使用する上記ＳＡの構成の候補を送信し、該ネットワーク接続装置９０３は上記候補の中から受け入れ可能なＳＡを返信するものである。ここで、上記ＳＡの構成の候補は、上記ネットワーク接続装置９０２のデータ記憶部に予め記憶されている認証アルゴリズム、暗号化アルゴリズム等を用いて構成される。上記ネットワーク接続装置９０２がどの様な認証アルゴリズム、暗号化アルゴリズムを搭載しているかは、ネットワーク接続装置により異なる。また、予め上記ネットワーク接続装置９０２が提案するＳＡを決めておくことも可能である。

【００２０】

上記ＳＡの返信処理により、ＩＰＳＥＣ通信に使用されるＳＡが確立される。

上記確立されたＩＰＳＥＣ通信に使用されるＳＡの情報は、図１２に示すＳＡＤ１２０１及び、図１１に示すＳＰＤ１１０１に格納される。該ＳＰＤ１１０１の構成は以下の例に示される。即ち、受信アドレス１１０２、ＩＰＳＥＣ処理の有無１１０３、上記ＳＡＤ１２０１における各ＳＡの位置を示すアドレスポインタ１１０４、及び上記受信ホストアドレス１１０２にデータを送信する場合に、ＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス１１０５である。ここで、上記ＩＰアドレス１１０５は、具体的にはネットワーク接続装置９０３のＩＰアドレスとなる。又、送信先の通信端末がＩＰＳＥＣ機能を搭載している場合、上記ＩＰアドレス１１０２が上記ＩＰアドレス１１０５と同一となる。さらに、上記受信ホストアドレス１１０２及びＩＰアドレス１１０５は範囲指定が可能である。範囲指定とは、具体的にはＩＰアドレスを用いて例えば”１９２．１６８．１．１～１９２．１６８．１．１００”という指定を指し、上記範囲指定により１つの指定で例えば２００台の通信端末へのデータの送信を指定することが出来る。尚、上記ＳＡは片方向で１つ設定されるので、双方通信の場合は独立したＳＡがネットワーク接続装置９０２、９０３にそれぞれ設定されることになる。

【００２１】

上記ＩＰＳＥＣ通信に使用されるＳＡが確立された後、送信側（元）のコンピュータ９０１から上記コンピュータ９０４に送信されるデータは、該コンピュータ９０１にてＩＰヘッダを付加され、ＩＰパケットとしてＬＡＮ９０７を介してネットワーク接続装置９０２に送られる。該ネットワーク接続装置９０２は、後述するＩＰＳＥＣ処理を行うことにより上記ＩＰパケットをＩＰＳＥＣパケット１００３として、上記ネットワーク接続装置９０３に送信する。上記ＩＰＳＥＣパケット１００３を受信した上記ネットワーク接続装置９０３は、同じく後述するＩＰＳＥＣ処理にて上記ＩＰＳＥＣパケット１００３をＩＰパケットに戻し、上記ＬＡＮ９０８を介して上記コンピュータ９０４に送信する。即ち、上記インターネット９０９を介して接続される上記ネットワーク接続装置９０２、９０３間では、送信側のコンピュータ９０１から上記コンピュータ９０４に送信されるデータはＩＰＳＥＣによりセキュリティが確保されるに至る。

【００２２】

続いて、図９、図１３、図１４を用いて上記ネットワーク接続装置９０２及び９０３におけるＩＰＳＥＣ処理の詳細を説明する。但し、機器構成や採用する方法によって様々な処理が行われるため、ここではその一例のみを示す。ここに図１３は、送信側ネットワーク接続装置におけるＩＰＳＥＣ処理のフローチャート、図１４は、受信側ネットワーク接続装置におけるＩＰＳＥＣ処理のフローチャートである。尚、後述するＳＰＤ、ＳＡＤはそれぞれのネットワーク接続装置内のデータ記憶部に記憶されている。ここで、図１３、１４におけるＳはステップを意味する。

【００２３】

上記ネットワーク接続装置９０２では、送信側のコンピュータ９０１より送信されたＩＰパケットを受信すると、まずその受信ホストアドレスを読み出す（図１３：Ｓ１３０１）。つづいて該受信ホストアドレスを基に上記ネットワーク接続装置９０２に格納される上記ＳＰＤ１１０１の受信ホストアドレス１１０２を検索し、対応するＩＰＳＥＣパケットを送信すべき先の通信端末のＩＰアドレス１１０５、ＩＰＳＥＣ処理の有無１１０３及びＳＡの位置を示すアドレスポインタ１１０４を読み出す（図１３：Ｓ１３０２）。

【００２４】

ここで、ＩＰＳＥＣ処理を行わない設定、即ちＩＰＳＥＣ処理の有無１１０３が”無”の場合、上記受信したＩＰパケットをそのまま上記ネットワーク接続装置９０３に送信する（図１３：Ｓ１３０３のＮｏ）。

【００２５】

ＩＰＳＥＣ処理を行う設定、即ちＩＰＳＥＣ処理の有無１１０３が”有”の場合、更に上記ＳＡの位置を示すアドレスポインタ１１０４を用いて上記ＳＡＤ１２０１を検索し、該当するＳＡの内容を読み出す（図１３：Ｓ１３０３のＹｅｓ→Ｓ１３０５）。該ＳＡは、上記ＩＫＥフェーズ２（図１０：Ｓ１００２）で確立されたＳＡである。次に、上記ネットワーク接続装置９０２は、上記ＳＡの内容に従い、例えば認証アルゴリズムとしてＨＭＡＣ－ＭＤ５－９６等を、暗号化アルゴリズムとしてＤＥＳ－ＣＢＣ等を用いて上記ＩＰパケットから認証／暗号

化データを作成する（図１３：Ｓ１３０５）。さらに、上記ネットワーク接続装置９０２は、上記認証／暗号化データに、認証ヘッダＡＨ(Authentication Header)または認証／暗号化ヘッダＥＳＰ(Encapsulation Security Payload)ヘッダを追加し、ＩＰＳＥＣ処理を施したＩＰパケット（ＩＰＳＥＣパケット１００３）とする（図１３：Ｓ１３０６）。

【００２６】

ここで、上記ＡＨ及びＥＳＰには上記ＩＫＥフェーズ２で確立したＳＡを構成する上記ＳＰＩ１２０８が含まれる。続いて上記ＩＰＳＥＣパケット１００３は、インターネット９０９を介して上記ＳＰＤ１１０１のＩＰアドレス１１０５が示す上記ネットワーク接続装置９０３に送信される。

【００２７】

次に、上記ネットワーク接続装置９０３は、受信したＩＰパケットがＩＰＳＥＣパケットであるかを判別する（図１４：Ｓ１４０１）。

【００２８】

ここで、ＩＰＳＥＣパケットでない場合、上記ＩＰパケットはそのままＬＡＮ９０８を介してコンピュータ９０４に送信される（図１４：Ｓ１４０１のＮｏ）。

【００２９】

受信したＩＰパケットが、ＩＰＳＥＣパケットである場合、以下の処理を行う（図１４：Ｓ１４０１のＹｅｓ）。即ち、まず上記ＩＰＳＥＣパケット内の上記ＡＨやＥＳＰヘッダを調べ、該ＡＨやＥＳＰヘッダに含まれるＳＰＩを読み出す（図１４：Ｓ１４０２）。次に、上記ネットワーク接続装置９０３に格納されるＳＡＤを上記ＳＰＩを用いて検索し、上記ＳＰＩに該当する、上記ＩＫＥフェーズ２で確立したＳＡの内容を読み出す（図１４：Ｓ１４０３）。これにより、上述したＩＫＥフェーズ２で確立した該当ＳＡが読み出されることになる。ここで、Ｓ１４０２にて該当ＳＰＩが無い場合はユーザにその旨を表示して処理を終了する（図示せず）。

【００３０】

さらに、上記ネットワーク接続装置９０３は、上記読み出したＳＡで指定され

た認証／暗号化アルゴリズム等を用いて、上記ＩＰＳＥＣパケットの認証／暗号化データを認証／復号化する（図１４：Ｓ１４０４）。又、必要に応じて上記ＳＡのアドレス１１０４を用いてＳＰＤ１１０１を検索し、送信（元）ホストのＩＰアドレス及び、ＩＰＳＥＣ処理の有無を確認し、元のＩＰパケットを生成する（図１４：Ｓ１４０５→１４０６）。続いて上記ネットワーク接続装置９０３は生成した上記ＩＰパケットをコンピュータ９０４に送信する。

【００３１】

以上により、上記認証／復号化された上記ＩＰＳＥＣパケットの認証／暗号化データは、ＩＰパケットとしてＬＡＮ９０８を介してコンピュータ９０４に送信される。即ち、上記ネットワーク接続装置９０２、９０３間では、送信側のコンピュータ９０１から上記コンピュータ９０４に送信されるデータはＩＰＳＥＣにてセキュリティが確保される。

【００３２】

以上がＩＰＳＥＣについての詳細な処理内容であるが、上記処理に加えて、より一層秘匿性の高い通信を実現するために、以下のような処理が行われる。即ち、上記ＳＡ１２０２～１２０４に「ライフタイム」と呼ばれる有効期間を設けるものである。

【００３３】

例えば所定の通信端末と長時間の通信を行う場合には、第３者に通信中の情報を盗聴し、解析する時間を与えてしまい、即ち情報漏洩の可能性が高くなってしまう。このようなケースでは、上記ＳＡに有効期間を設け、所定の時間間隔を持って再度新たなＳＡを確立することで秘匿性を高めるのである。

【００３４】

即ち、図１５に示すように、ＳＡ１（１５０１）は、所定の時間（例えば８時間）の有効期間を有する。当該有効期間の情報は、図１２に示した有効期間１２１０に格納されている。また、上記ＳＡ１（１５０１）が確立（作成、登録）された時刻１５０２が登録時刻１２０９に格納されている。上記登録時刻１２０９と有効期間１２１０により、ＳＡ１（１５０１）が通信に利用される最終時刻１５０３が決定される。即ち、上記ＳＡ１（１５０１）の有効期間が過ぎると次に

例えばＳＡ５（１５０４）が対応する通信端末との通信に利用されることになる。

【００３５】

但し、上記ＳＡ５（１５０４）の確立には、上述したようなＩＫＥを用いた複雑な手順が必要となるために、多少の時間１５０５を要する。よって、上記更新待ち期間１２１１に、例えば最終時刻１５０３からの時間１５０６や、ＳＡ１（１５０１）確立時からの時間１５０７等を格納することにより、当該更新待ち期間１２１１が示す時刻１５０８よりＳＡ５（１５０４）確立の為の処理を開始している。

【００３６】

尚、新たなＳＡ５（１５０４）が確立された後は、古いＳＡ１（１５０１）は有効期間終了時刻の到来をもって上記ＳＡＤから削除されるに至る。

【００３７】

【発明が解決しようとする課題】

上述したように、例えば上記ＩＰＳＥＣを用いることにより、秘匿性の高い通信が実現できるわけである。しかしながら、上述した処理、特に図１４のＳ１４０３に示したＳＡを検索する処理は基本的にパケットの送受信毎に行われる。従来では、ＩＰＳＥＣ等におけるボトルネック処理は、暗号化／復号化処理と認証処理であったが、近年、暗号／復号、認証処理のハードウェア化が進行しており、そのボトルネックが解消される方向にある。そのような場合、次に問題となるボトルネック処理としては、上記ＳＡＤの検索処理が挙げられる。特に、ネットワークの通信量が増大し、各端末のパケット処理量が増加すると、この影響が顕著に現れる。さらに、コネクションを集群する基幹ルータなどでは、その影響は特に深刻な問題である。

【００３８】

さらに上記ＳＡの有効期間は、当該ＳＡに対応するパケットの、入出力時におけるＳＡ検索でのみ検査される。このため、パケットの入出力が中断している期間に、上記ＳＡの有効期間が過ぎている場合には、それらの時間を検知する方法がない。従って、通信を一時中断している間にＳＡの有効期間が終了していると

、通信の再開時にまず送受信端でＳＡの確立をしなければならず、通信が迅速に再開できないといった問題がある。

【００３９】

また、ＩＰＳＥＣプロトコルを用いて長時間のリアルタイム映像通信を行う場合には、通信中にＳＡの有効期間が過ぎることがあり、当該通信途中に上記ＩＫＥプロトコルで新たなＳＡを確立した後に新ＳＡを有効化する場合がある。しかしながら、例えばインターネットのようなネットワークでは、不特定の通信経路が利用されるため、パケットの到着順序が保証されるものではない。従って、受信端末のＳＡは新ＳＡになっているのにもかかわらず、旧ＳＡを適用したパケットが受信端末により受信されるといった状態が発生し得る。

【００４０】

このような状態が発生した場合、上記ＳＡＤ内の新ＳＡと旧ＳＡとの検索時間の差により、受信した映像にブランクや乱れが生じる。

【００４１】

さらに、有効期間の終了間際に、パケットが送信端から出力された場合には、受信端末にパケットが届く時間にはＳＡの有効期間が終了しており、そのパケットは破棄されてしまうといった問題も生じる。

【００４２】

従って本発明は、有効期間を有するデータベースの管理装置、管理方法及びその記録媒体において、当該データベース内の検索対象となるデータを短時間に検索すると共に、有効期間の終了するデータと当該データの後継データとの切換をスムーズに行うデータベース管理装置、管理方法及びその記録媒体を提供することを目的とするものである。

【００４３】

【課題を解決するための手段】

本発明は、上記目的を達成するために以下の手段を備える。

【００４４】

すなわち、有効期間を含む必要事項より構成される情報を一データ単位とし、当該データの有効期間が終了するに際して該データに対応する後継データを作成

するデータベース管理装置を前提としている。ここで、関連情報追加手段は、有効期間が終了する所定のデータと、これに対応する後継データとの両方又はどちらか一方に関連情報を追加する。

【００４５】

以上により、一方のデータが検索された場合に、関連する他方のデータを瞬時に読み出すことが可能になる。従って、目的とするデータを検索する速度を高めるとともに、データベース管理装置の負荷を下げることができる。

【００４６】

尚、関連情報検索手段が、所定のデータ又は後継データの参照時に、当該データに含まれる上記関連情報を参照して対応するデータを検索する。

【００４７】

又、有効期間管理手段が、有効期間と、当該有効期間を含むデータの参照情報とを関連付けて記憶すると共に、有効期間の終了に際してその旨を通知し、通知を受けた、データ制御手段が上記データに対して当該有効期間終了に伴う所定の処理を行う構成がある。尚、所定の処理が、上記対応する後継データの作成や、上記有効期間が終了するデータの削除である構成がある。

【００４８】

この構成では、データの作成、登録や削除等、必要な処理を確実に行うことができる。上記必要な処理を確実に行うことにより、不要なデータを放置することによる検索速度の低下や記憶領域の無駄を防ぐことが可能となる。

【００４９】

さらに、上記情報が、上記有効期間が終了する前に上記後継データを作成すべき時間情報を含むに際して、時間情報と、当該時間情報を含むデータの参照情報とを関連付けて記憶すると共に、当該時間情報にて示された時間の到来を通知する更新管理手段と、この通知を受けて、後継データを作成する構成がある。尚、この構成において、有効期間が終了する所定のデータと、当該所定のデータに対応する後継データとの両方又はどちらか一方に上記データを相互に関連付けた関連情報を追加する関連情報追加手段を備えてもよい。

【００５０】

更新開始時刻を正確に管理することで、確実に後継データを作成、登録することが可能になる。また、更新待ち期間に十分な余裕を持たすことにより、データと後継データの何れかが常時有効な状態で存在することになり、データの作成、登録のための通信の遅延を確実に無くすことができる。

【００５１】

又、有効期間の終了を延長する延長期間情報を記憶すると共に、上記有効期間が終了するに際して、当該有効期間が終了するデータの有効期間を上記延長期間情報が示す期間延長する有効期間延長手段を具備する構成や、後継データの作成時に、後継データの検索順序を、該後継データに対応するデータの前方に位置させる検索順序管理手段を備える構成もある。

【００５２】

有効期間延長手段を設けることで、本来破棄されるデータ（パケット）を破棄することなく活用することができる。

【００５３】

さらに、上記後継データと該後継データに対応するデータの検索頻度を監視する検索頻度監視手段を備え、検索順序管理手段が、検索頻度に基づいて所定のデータと後継データの検索順序を変更する構成がある。

【００５４】

この構成では、後継データと当該後継データに対応するデータがどちらも検索される期間において、２つのデータのうち検索頻度が高いデータを検索時間の短い検索順序に設定することで、検索頻度の高いデータを短時間で検索することが可能になる。尚、上記データは、ＩＰＳＥＣ(Internet Protocol Security Protocol) 通信に用いられるＳＡ（Security Association）としてもよい。

【００５５】

【発明の実施の形態】

以下、添付図面を参照して、本発明の実施の形態につき説明し、本発明の理解に供する。尚、以下の実施の形態は、本発明を具体化した一例であって、本発明の技術的範囲を限定する性格のものではない。

【００５６】

〔実施の形態１〕

まず、図１、図２、図９を用いて本実施の形態１におけるデータベース管理装置の構成の概略を説明する。尚、上記データベース管理装置１０１は、図９に示したネットワーク接続装置９０２、９０３やコンピュータ９０１であって、例えばＩＰＳＥＣ機能を実装する端末内に設けられる。ネットワークの構成においては、図９における従来技術と同様の構成を用いて説明する。

【００５７】

上記ネットワーク接続装置９０２及び９０３は、一般的に図２に示すような構成を有する。即ち、処理部２０１、一時データ記憶部２０２、データ記憶部２０３、システム制御部２０４、ネットワーク制御部２０６、回線制御部２０７が内部バス或いはスイッチ２０５にてそれぞれ接続されている。また、上記ネットワーク制御部２０６は例えば上記ＬＡＮ９０７に、上記回線制御部２０７はインターネット９０９とそれぞれ接続されている。尚、本実施の形態１ではネットワーク接続装置９０２及び９０３は、ネットワーク制御部２０６と回線制御部２０７を１個づつ具備した構成であるが、ネットワーク制御部２０６のみが複数個ある構成でも構わない。

【００５８】

従来技術にて示したＳＰＤ、ＳＡＤは、フラッシュメモリ、ハードディスク、ＲＯＭ等の不揮発性メモリで構成された上記データ記憶部２０３に格納される。上記処理部２０１は、上記ネットワーク接続装置９０２の電源投入時に上記データ記憶部２０３からシステム制御部２０４を経由して、上記ＳＰＤ，ＳＡＤを読み出し、ＤＲＡＭ、ＳＲＡＭ等の揮発メモリで構成される上記一時データ記憶部２０２に格納するかあるいは、必要なときに読み出し、一時データ記憶部２０２に格納する。又、上記ＳＰＤ、ＳＡＤの更新は、上記データ記憶部２０３及び、一時データ記憶部２０２に格納されているＳＰＤ、ＳＡＤに対して行なわれる。

【００５９】

即ち、図１に示すデータベース管理装置１０１は、上記処理部２０１にて実行され、例えばソフトウエアやハードウェアとして提供される。また、ＳＡＤ１０２は、上記データ記憶部２０３、一時データ記憶部２０２等に記憶されている。

従って、ＳＡＤシステム１０３は、上記処理部２０１、データ記憶部２０３及び／又は一時データ記憶部２０２により構成される。

【００６０】

尚、従来技術にて説明したように、ＬＡＮ９０７或いはインターネット９０９からそれぞれネットワーク制御部２０６、回線制御部２０７を経由して受信した個々のＩＰパケット（ＩＰＳＥＣパケット）は、上記処理部２０１にて上述したＩＰＳＥＣ処理が行われる。即ち、上記処理部２０１は、個々のＩＰＳＥＣパケットの上記ＡＨ、ＥＳＰ情報を読み出し、上述した処理フローに従って上記一時データ記憶部２０２に格納された必要なＳＰＤ、ＳＡＤを検索してＩＰＳＥＣに関する認証／暗号化、認証／復号化を行った後、送信先アドレスに送信する。また、その他の機能（ルーティング機能等）も上記処理部２０１にて提供される。

【００６１】

ここで、個々のＩＰパケット処理時に、一時データ記憶部２０２に格納されたＳＰＤ、ＳＡＤを検索する理由は、上記一時データ記憶部２０２がデータ記憶部２０３に比べて高速にアクセス可能であり、上記ＩＰＳＥＣ処理の高速化を図ることができるためである。

【００６２】

次に、図１、図３を用いて本実施の形態１におけるデータベース管理装置１０１の処理の詳細について説明する。

【００６３】

データベース管理装置１０１を構成するＳＡＤ制御手段１０４は、有効期間におけるＳＡの削除、交換、更新開始時間における挿入、検索およびその要素の設定などを行うが詳細は後述する。尚、上記処理はその一例を示したのみであり、その他の処理を行っても構わない。

【００６４】

また、ＳＡＤ内の各ＳＡ（図１のＳＡ１～ＳＡ５）の要素（必要事項）としては、送信ホストアドレス１１２、受信ホストアドレス１１３、プロトコル１１４、ＳＰＩ１１５、登録時刻１１６、有効期間１１７、更新待ち期間１１８、関連ＳＰＩ有無情報１１９、関連ＳＰＩ１２０および相互参照情報１２１がある。な

お、前記ＳＡの要素はその一例を示したが、その他、従来技術にて示した認証アルゴリズム１２１２、認証鍵１２１３、暗号化アルゴリズム１２１４、暗号化鍵１２１５等の情報を有していても構わなし、先に挙げた要素の中で不要なものは持たなくても構わない。

【００６５】

以上が本実施の１形態で取り扱うＳＡＤシステム１０３の基本構成である。

【００６６】

以降、本実施の形態１を、ＳＡ１（１１１）が有効期間の終了に達し、ＳＡ５１３１がＳＡ１（１１１）の有効期間後のＳＡとなる場合を用いて説明を行う。尚、上記ＳＡＤ内の各ＳＡの検索順序は、例えば各ＳＡが作成された順序や、当該ＳＡが記憶されている記憶領域のアドレス順に従って決定されるものである。又、本実施の形態１においては、上記有効期間の終了の管理については特に問題とならないため省略する。

【００６７】

まず、上記データベース管理装置１０１は、ＳＡ１（１１１）の有効期間が終了し、又は終了近くなると上記ＳＡ１（１１１）の後継ＳＡとなるＳＡ５（１３１）を作成する。尚、当該ＳＡ５（１３１）は、上述したＩＫＥプロトコルを用いて相手側の通信端末と通信を行うことにより、当該ＳＡ５に格納する必要事項を決定した後作成される。ここで、上記データベース管理装置１０１を構成する関連情報追加手段１０５は、当該ＳＡ１（１１１）に、関連ＳＰＩ有無情報１１９、関連ＳＰＩ１２０、相互参照情報１２１を追加する。

【００６８】

上記関連ＳＰＩ有無情報１１９には、関連する（即ち後継ＳＡである）ＳＡ５（１３１）の存在の有無、即ち後述する関連ＳＰＩ１２０及び相互参照情報１２１の”有効”、”無効”を示すフラグが格納される。上記ＳＡ５（１３１）が作成されるまでは当該関連ＳＰＩ有無情報１１９には”無効”を示す情報が格納されることになる。又、上記関連ＳＰＩ１２０には、ＳＡ５（１３１）にて格納されているＳＰＩ１３５が、相互参照情報１２１には上記ＳＡ５の場所情報、即ち、ＳＡ５が格納される領域のアドレスを示すポインタが格納される。

【００６９】

さらに、ＳＡ５（１３１）において、関連ＳＰＩ有無情報１３９には、関連するＳＡ１（１１１）の存在の有無、即ち関連ＳＰＩ１４０及び相互参照情報１４１の”有効”、”無効”を示すフラグが格納される。又、上記関連ＳＰＩ１４０には、ＳＡ１（１１１）にて格納されているＳＰＩ１１５が、相互参照情報１４１には上記ＳＡ１（１１１）のアドレスを示すポインタが格納される。

【００７０】

以上の関連ＳＰＩ有無情報１１９、１３９、関連ＳＰＩ１２０、１４０、相互参照情報１２１、１４１により、例えばＳＡ１（１１１）がＳＡＤ制御手段１０４にて検索された場合にはＳＡ５（１３１）の位置を、又、ＳＡ５（１３１）が検索された場合にはＳＡ１（１１１）の位置を直ちに読み出すことが可能になる。

【００７１】

続いて、図１、図３を用いて上記データベース管理装置１０１が、上記ＳＡＤ１０２内のＳＡを検索する手順について説明する。

【００７２】

上記ＳＡＤ制御部１０４は、パケットの送受信時に、必要に応じてＳＡＤ１０２内のＳＡを順次検索し、目的とするＳＡを見つけるとその内容を読み出す。ここでは、例えばＳＡ５（１３１）を適用したＩＰＳＥＣパケットが入力された場合の、ＳＡ５（１３１）の読み出しまでの例を説明する。

【００７３】

まず前記ＩＰＳＥＣのヘッダ情報より、受信ホストアドレス、プロトコルおよびＳＰＩを検索条件として抽出する。次に、ＳＡＤ内の全ＳＡを検索したかを確認し、もし全ＳＡの検索が終了している場合には検索を誤終了する（図３：Ｓ３０１ＹＥＳ→Ｓ３０９）。

【００７４】

上記全ＳＡを検索したかを確認する処理において、まだ検索していないＳＡが有る場合には次の処理を行う（図３：Ｓ３０１ＮＯ→Ｓ３０２）。ここでは最初の検索であるために、次の処理を行う。

【００７５】

続いて、上記抽出した受信ホストアドレス、プロトコルと、ＳＡ１内の受信ホストアドレス１１３、プロトコル１１４とを比較する（図３：Ｓ３０２）。

【００７６】

尚、上記抽出した受信ホストアドレス、プロトコルと、ＳＡ１内の受信ホストアドレス１１３、プロトコル１１４が一致しなければ次のＳＡに検索処理を移す（図３：Ｓ３０２ＮＯ→Ｓ３０８→Ｓ３０１）。

【００７７】

ここで、上記抽出した受信ホストアドレス、プロトコルと、ＳＡ１内の受信ホストアドレス１１３、プロトコル１１４が一致する場合、さらに上記抽出したＳＰＩとＳＡ１（１１１）のＳＰＩ１１５を比較する（図３：Ｓ３０２ＹＥＳ→Ｓ３０３）。

【００７８】

上記抽出したＳＰＩとＳＡ１（１１１）のＳＰＩ１１５が等しい場合、当該ＩＰＳＥＣパケットが目的とするＳＡであるために、当該ＳＡの内容を読み出して検索終了となる（図３：Ｓ３０３ＹＥＳ→Ｓ３０５）。

【００７９】

尚、ここでは、ＳＡ５（１３１）が検索対象であるために、上記抽出したＳＰＩはＳＰＩ１１５と一致しない。従って、次に関連ＳＰＩ有無情報１１９の内容を確認する（図３：Ｓ３０３ＮＯ→Ｓ３０４）。

【００８０】

続いて、上記関連ＳＰＩ有無情報１１９が関連ＳＰＩの存在を示していない、即ち内容が”無効”である場合、次のＳＡに検索処理を移す（図３：Ｓ３０４ＮＯ→Ｓ３０８→Ｓ３０１）。上記”無効”は、後継ＳＡが無いことを示し、これは通常通信時であって、未だＳＡ１（１１１）が十分な有効期間を有する場合を示す。

【００８１】

ここで、上記関連ＳＰＩ有無情報１１９が関連ＳＰＩの存在を示している、即ち内容が”有効”である場合、上記抽出したＳＰＩとＳＡ１（１１１）の関連Ｓ

ＰＩ１２０とを比較する（図３：Ｓ３０４ＹＥＳ→Ｓ３０６）。

【００８２】

上記抽出したＳＰＩとＳＡ１（１１１）の関連ＳＰＩ１２０が異なる場合、当該ＳＡ１（１１１）はＳＡ５（１３１）とは関連しないとして、次のＳＡに検索処理を移す（図３：Ｓ３０６ＮＯ→Ｓ３０８→Ｓ３０１）。

【００８３】

ここで、上記抽出したＳＰＩとＳＡ１（１１１）の関連ＳＰＩ１２０が等しい場合、当該ＳＡ１（１１１）は後継ＳＡを有し、当該後継ＳＡの参照情報が相互参照情報１２１に格納されていることを意味するので、当該相互参照情報１２１に格納されている参照情報（ポインタ）を用いてＳＡ５（１３１）を決定する（図３：Ｓ３０６ＹＥＳ→Ｓ３０７）。続いて、上記ＳＡ５（１３１）が格納する必要事項より構成される情報を読み出して、検索は正常終了となる（図３：Ｓ３０７→検索正常終了）。

【００８４】

以上の処理にて読み出された各ＳＡに格納される必要事項が、当該ＩＰＳＥＣパケットの暗号化の解除（復号化）等に利用されるのは従来技術と同様である。尚、上記関連ＳＰＩ有無情報、関連ＳＰＩ、相互参照情報を参照する処理（Ｓ３０４、Ｓ３０６、Ｓ３０７）は、上記ＳＡＤ制御手段１０４を構成する関連情報検索手段１０６にて行われる。

【００８５】

以上のように、従来ではＳＡ１が検索対象でない場合には、例えばＳＡ２、ＳＡ３といった順に検索を行う必要があったが、関連ＳＰＩ有無情報、関連ＳＰＩ、相互参照情報といったデータ間の関連情報をそれぞれのデータに設けることにより、一方のデータが検索された場合に、関連する他方のデータを瞬時に読み出すことが可能になる。これにより、目的とするＳＡを検索する速度を高めるとともに、データベース管理装置の負荷を下げることができる。

【００８６】

尚、本実施の形態１では、ＳＡの関連情報を上記関連ＳＰＩ有無情報、関連ＳＰＩ、相互参照情報の３つにしたが、その他の情報を有していても構わなし、不

要なものは必ずしも必要ない。又、本実施の形態ではＳＡから関連するＳＡへの参照方法に格納領域のアドレス（ポインタ）を用いたが、データベースが管理するデータのエントリ番号等を用いても構わない。

【００８７】

又、上記ＳＡの検索手順では、ＳＰＩ以外の検索条件に受信ホストアドレス、プロトコルを用いたが、これらに加えてパケットの優先処理フラグ（ＩＰｖ４では”Type of Service ”フィールド、ＩＰｖ６では”Flow Label”フィールド）を検索条件に加えても構わないし、必要な場合にはその他の情報を検索条件に加えてもよい。

【００８８】

〔実施の形態２〕

次に、図４、図５を用いて本実施の形態２におけるデータベース管理装置４０１の構成を説明する。尚、上記データベース管理装置４０１は上記実施の形態１と共通点が多いため、異なる点のみ説明する。又、ＳＡＤ１０２に記憶される各ＳＡ（ここではＳＡ１～ＳＡ５）には、登録時刻１１６、１３６、有効期間１１７、１３７、更新待ち期間１１８、１３８がそれぞれ格納されるが、例えば上記実施の形態１にて説明した関連ＳＰＩ有無情報、関連ＳＰＩ、相互参照情報等の関連情報は必ずしも必要ではない。また、更新待ち時間１１８、１３８も必ずしも必要ではない。ここで、上記ＳＡ１（１１１）の登録時刻１１６には、図５に示す、当該ＳＡ１（１１１）が作成された登録時刻５０１の値が格納される。又、上記有効期間１１７には当該ＳＡ１（１１１）が通信において使用可能な有効期間５０２が格納される。さらに、更新待ち期間１１８には、上述したＩＫＥプロトコルを用いた後継ＳＡの作成に必要な時間５０５にある程度余裕を持たせた時間（図５に示す更新待ち期間５０３）が格納される。但し、上記登録時刻１１６、有効期間１１７、更新待ち期間１１８は、上記図５における登録時刻５０１、有効期間終了時刻５０５、及び更新開始時刻５０６を特定できるものであればよく、時刻や時間、その他の異なる型式の情報として格納してもよい。ここに更新開始時刻とは、例えば上記ＩＫＥプロトコルを用いた通信を開始する時刻である。

【００８９】

本実施の形態２におけるデータベース管理装置４０１は、さらに有効期間管理手段４０２を備える。当該有効期間管理手段４０２には、各ＳＡ１～５に対応する有効期間管理情報４１０～４１４が格納される。当該有効期間管理情報４１０～４１４には、対応するＳＡ１～５の位置情報（ポインタ）が参照情報として、又、対応するＳＡ１～５の有効期間終了時刻（例えば図５の５０５）が有効期間終了時刻として格納される。尚、上記有効期間管理情報は、当該ＳＡの登録時に当該有効期間管理手段４０２により登録される。上記有効期間管理情報４１０～４１４は、イベントキューの形で格納されており、有効期間終了時刻の早い順に並んでいるものとする。尚、上記参照情報はポインタに限らず、データベースにおけるエントリ番号等、上記ＳＡ１～５を特定して参照可能な情報であればよい。

【００９０】

続いて図４を用いて、上記有効期間管理手段４０２の処理の詳細を説明する。

【００９１】

上記有効期間管理手段４０２を構成するイベント起動部４０３は、ＳＡ１が作成された旨を示す情報をＳＡＤ制御手段４０５から受け取ると、当該ＳＡ１に対応する有効期間管理情報４１０を有効期間管理手段４０２内に格納する。有効期間管理情報の内容は上述した通りであるが、有効期間終了時刻は当該登録時点においてＳＡ１内に格納されている登録時刻１１６及び有効期間１１７を用いて算出される。以後、同様に順次ＳＡ２～ＳＡ４に関しても有効期間管理情報４１１～４１３が格納される。

【００９２】

続いて、上記有効期間管理情報４１０が格納されると、当該有効期間管理情報４１０を構成する有効期間終了時刻は、イベント起動部にて読み込まれ、該イベント起動部４０３は上記有効期間終了情報を計時部４０４に設定する。

【００９３】

上記計時部４０４は、常時時刻を監視し、上記ＳＡ１に対応する有効期間終了時刻が来ると上記イベント起動部４０３に通知する。

【００９４】

上記通知を受けると、イベント起動部４０３は上記有効期間管理情報４１０を参照し、ＳＡ１の参照情報を読み出してＳＡＤ制御手段４０５に当該参照情報を送信すると共に、続くＳＡ２に対応する有効期間管理情報４１１について計時部４０４への設定を行う。

【００９５】

上記参照情報を受信したＳＡＤ制御手段４０５は、当該参照情報に基づいてＳＡ１を削除する。又、同時にＳＡ１に対応する後継ＳＡである、ＳＡ５の作成、登録処理を行ってもよい。

【００９６】

以上のように、従来では、所定の時刻に当該ＳＡに関するパケットの入出力が無い場合には当該ＳＡに対して作成、登録や削除処理等が行われたかったが、ＳＡの有効期間を管理するための機能を付加することで、ＳＡの作成、登録や削除等、必要な処理を確実に行うことができる。上記必要な処理を確実に行うことにより、不要なＳＡを放置することによる検索速度の低下やＳＡＤの記憶領域の無駄を防ぐことが可能となる。

【００９７】

尚、上記実施の形態１にて説明した関連情報を上記実施の形態２における各ＳＡに追加するとともに、ＳＡＤ制御手段１０４を構成する関連情報検索手段１０６、関連情報追加手段１０５を上記ＳＡＤ制御手段４０５に採用することにより、ＳＡの検索速度をより一層高速化することが可能となる。

【００９８】

〔実施の形態３〕

次に、図５、図６を用いて本実施の形態３におけるデータベース管理装置６０１について説明する。尚、本実施の形態３におけるデータベース管理装置６０１は上記実施の形態２と共通点が多いため、異なる点のみ説明する。又、ＳＡＤ１０２に記憶される各ＳＡ（ここではＳＡ１～ＳＡ５）には、登録時刻１１６、１３６、有効期間１１７、１３７、更新待ち期間１１８、１３８がそれぞれ格納されるが、例えば上記実施の形態１、２にて説明した関連ＳＰＩ有無情報、関連Ｓ

ＰＩ、相互参照情報等の関連情報は必ずしも必要ではない。

【００９９】

本実施の形態３におけるデータベース管理装置６０１は、上記実施の形態２にて説明した有効期間管理手段４０２を備える。但し、当該有効期間管理手段４０２には、有効期間管理情報４１０～４１４に加えて、更新開始時刻情報６１１～６１３が格納される。当該更新開始時刻情報６１１～６１３には、対応するＳＡ１～５の位置情報（ポインタ）が参照情報として、又、対応するＳＡ１～５の更新開始時刻（例えば図５の５０６）が更新開始時刻として格納される。尚、上記情報は、当該ＳＡの登録時に当該有効期間管理手段４０２により登録される。上記更新開始時刻情報６１１～６１３も、イベントキューの形で格納されており、更新開始時刻、及び有効期間終了時刻の早い順に並んでいるものとする。即ち、通常、例えばＳＡ１に関する更新開始時刻情報６１１の次にＳＡ１に関する有効期間管理情報が格納される。

【０１００】

続いて図６を用いて、上記有効期間管理手段４０２の処理の詳細を説明する。

【０１０１】

上記有効期間管理手段４０２を構成するイベント起動部４０３は、ＳＡ１が作成された旨を示す情報をＳＡＤ制御手段４０５から受け取ると、当該ＳＡ１に対応する更新開始時刻情報６１１を有効期間管理手段４０２内に格納し、続いて有効期間管理情報４１０を有効期間管理手段４０２内に格納する。

【０１０２】

更新開始時刻は当該登録時点においてＳＡ１内に格納されている登録時刻１１６、有効期間１１７、及び更新待ち期間１１８を用いて算出される。以後、同様に順次ＳＡ２～ＳＡ４に関しても更新開始時刻情報６１１～６１３、及び有効期間管理情報４１１～４１３が格納される。

【０１０３】

続いて、上記更新開始時刻情報６１１が格納されると、当該更新開始時刻情報６１１を構成する更新開始時刻は、イベント起動部にて読み込まれ、該イベント起動部４０３は上記更新開始時刻を計時部４０４に設定する。

【０１０４】

上記計時部４０４は、常時時刻を監視し、上記ＳＡ１に対応する更新開始時刻が来ると上記イベント起動部４０３に通知する。

【０１０５】

上記通知を受けると、イベント起動部４０３は上記更新開始時刻情報６１１を参照し、ＳＡ１の参照情報を読み出してＳＡＤ制御手段４０５に当該参照情報を送信すると共に、続く有効期間管理情報４１０について計時部４０４への設定を行う。尚、有効期間管理情報に対する有効期間管理手段の処理は上記実施の形態２にて示した通りである。

【０１０６】

上記参照情報を受信したＳＡＤ制御手段４０５は、当該参照情報に基づいて、ＳＡ１に対応する後継ＳＡであるＳＡ５を作成、登録するためのＩＫＥプロトコルを用いたネゴシエーションを行う。但し、当該ネゴシエーションはＩＰＳＥＣ通信にて利用される他の手段が行ってもよい。この場合には、上記ＳＡＤ制御手段４０５は、上記他の手段に当該ＳＡ１の情報及び上記ネゴシエーションを行う旨の指示を送信する。

【０１０７】

上記ＳＡＤ制御手段４０５がネゴシエーションを行う場合を仮定すると、当該ネゴシエーション終了後ＳＡ５が作成され、上記ＳＡＤ制御手段４０５は当該ＳＡ５（１３１）の登録時刻１３６に上記ＳＡ５（１３１）を作成、登録した時刻を格納し、さらにあらかじめ決められている有効時間１３７、更新待ち期間１３８も格納する。次に、当該作成した情報を上記有効期間管理手段４０２に通知し、当該有効期間管理手段４０２は、上記ＳＡ５に関する更新開始時刻情報６１３を登録するに至る。

【０１０８】

さらに、上記ＳＡＤ制御手段４０５は、上記実施の形態１にて説明した関連情報、即ち関連ＳＰＩ有無情報１１９、１３９、関連ＳＰＩ１２０、１４０、相互参照情報１２１、１４１にそれぞれ情報を格納する。又、同時に上記ＳＡ１（１１１）とＳＡ５（１３１）との検索順序を入れ換えてもよい。当該入れ替えの詳

細はＳＡＤの検索方法により異なるために割愛する。

【０１０９】

続いて、有効期間管理情報４１０の格納する有効期間終了時刻がくると、上記有効期間管理手段４０２は、その旨をＳＡＤ制御手段４０５に通知し、当該ＳＡＤ制御手段４０５は上記有効期間管理情報４１０に格納されている参照情報を基にＳＡ１（１１１）を削除する。又、当該削除に際して、関連するＳＡ５（１３１）の関連ＳＰＩ有無情報１３９を”無効”に書き換えると共に、関連ＳＰＩ１４０及び相互参照情報１４１の内容を消去する。

【０１１０】

以上のように、更新開始時刻５０６を正確に管理し、当該更新開始時刻には確実にＩＫＥプロトコルを用いたネゴシエーションを行うことにより、上記ＳＡ１に関するパケットが送受信されていない場合にも確実に後継ＳＡを作成、登録することが可能になる。また、更新待ち期間に十分な余裕を持たすことにより、ＳＡ１と後継ＳＡ５の何れかが常時有効な状態で存在することになり、ＳＡの作成、登録のための通信の遅延を確実に無くすことができる。

【０１１１】

さらに、上記十分な時間の余裕により、後継ＳＡであるＳＡ５が生成、登録された後もしばらくＳＡ１が存在するために、ＳＡ１を適用したＩＰＳＥＣパケットがネットワークの遅延等により遅れて到着した場合にも、当該パケットを破棄することなく正常に処理することが可能となる。これは、特に長時間のリアルタイム映像を送受信する場合等に、全てのパケットを問題なく処理でき、しかも関連情報により後継ＳＡまたはその元となるＳＡを瞬時に検索できるため、受信した映像にブランクや乱れを生じるにくくすることができる。

【０１１２】

尚、上記後継ＳＡの作成に関する更新開始時刻情報６１１～６１３を、有効期間管理手段と同様の機能を有する更新管理手段によりまとめて処理するようにしてもよい。

【０１１３】

〔実施の形態４〕

次に、図７を用いて本実施の形態４におけるデータベース管理装置７０１について説明する。尚、本実施の形態４におけるデータベース管理装置７０１は上記実施の形態１～３と共通点が多いため、異なる点のみ説明する。

【０１１４】

本実施の形態４では、ＳＡＤ制御手段１０４内に、有効期間延長手段７０２を備える。また当該有効期間延長手段７０２には、延長期間情報７０３が記憶されている。

【０１１５】

ＳＡ１（１１１）がＳＡＤ制御手段１０４にて検索されたにもかかわらず、上記ＳＡ１（１１１）を構成する有効期間１１７の情報が、既に有効期間を過ぎたものであった場合、上記有効期間延長手段７０２は、上記有効期間１１７の情報に上記延長期間情報７０３を加えた値を暫定有効期間とし、当該暫定有効期間に基づいてＳＡ１（１１１）の有効期間を判定する。

【０１１６】

ＳＡＤ制御手段１０４にて検索された時刻が、上記暫定有効期間内であった場合、当該ＳＡ１（１１１）を有効としＳＡ１を用いてパケットの符号化、復号化等を行う。

【０１１７】

通常、有効期間の終了間際に、パケットが送信端末から出力された場合には、受信端にパケットが届く時間にはＳＡの有効期間が終了しており、そのパケットは破棄されてしまうが、以上のように、有効期間延長手段を設けることで、本来破棄されるパケットを破棄することなく活用することができる。

【０１１８】

尚、上記延長期間情報は、通信先となる端末とのネットワーク構成やトラフィックを考慮して、通信先毎に独立して設けることで、通信状況に応じた設定が可能となる。

【０１１９】

〔実施の形態５〕

次に、図１、図８を用いて本実施の形態５におけるデータベース管理装置８０

１について説明する。尚、本実施の形態５におけるデータベース管理装置８０１は上記実施の形態１～４と共通点が多いため、異なる点のみ説明する。又、図１については、検索順序のみを参照する。

【０１２０】

本実施の形態５におけるデータベース管理装置８０１は、検索頻度監視手段８０２を備える。さらに、検索頻度監視手段８０２には、更新開始時刻が到来したＳＡ１と、そのＳＡの有効期間終了後にそのＳＡの後継ＳＡとなるＳＡ５への参照情報を持っている。

【０１２１】

以降、上記ＳＡ１の更新開始時刻が到来した後で、かつＳＡ１の有効期間が未だ終了しない間の状態、即ち図５における期間５１０の状態の場合の処理について説明する。尚、ＳＡ１（１１１）の後継ＳＡがＳＡ５（１３１）であるとする。

【０１２２】

まず、検索頻度監視手段８０２は、ＳＡ５（１３１）がＳＡ１（１１１）と関連のあるＳＡであることを更新開始時刻の処理にて認識し、ＳＡ１の検索回数とＳＡ５の検索回数の両方のカウントを開始する。次に、設定した所定の時間間隔で検索回数が多いＳＡを決定し、その後、参照情報８１０および８１１を用いて検索回数の多い順、例えばＳＡ５（１３１）の検索順序を図１の検索順序から図８に示す検索順序に変更する。即ち、検索順が、「ＳＡ１→ＳＡ２→ＳＡ３→ＳＡ４→ＳＡ５」であったのを「ＳＡ５→ＳＡ２→ＳＡ３→ＳＡ４→ＳＡ１」に変更する。尚、当該検索順序の変更の詳細はＳＡＤの検索方法により異なるために割愛する。

【０１２３】

なお、本実施の形態５では、検索回数が多いＳＡを早い検索順序に設定したが、ＳＡ１の有効期間後のＳＡであるＳＡ５を検索回数に関係なく、早い検索順序に設定しても構わない。

【０１２４】

以上により、後継ＳＡ（ＳＡ５）と当該後継ＳＡに対応するＳＡがどちらも検

索される期間において、２つのＳＡのうち検索頻度が高いＳＡを検索時間の短い検索順序に設定することで、検索頻度の高いＳＡを短時間で検索することが可能になる。

【図面の簡単な説明】

【図１】

本発明に係るデータベース管理装置及びＳＡＤの概略を示すイメージ図。

【図２】

本発明に係るデータベース管理装置を格納するネットワーク接続装置のハードウェアブロック図。

【図３】

本発明に係るデータベース管理装置の処理を示すフローチャート。

【図４】

実施の形態２におけるデータベース管理装置及びＳＡＤの概略を示すイメージ図。

【図５】

時間軸に対応するＳＡの状況を示す図。

【図６】

実施の形態３におけるデータベース管理装置及びＳＡＤの概略を示すイメージ図。

【図７】

実施の形態４におけるデータベース管理装置及びＳＡＤの概略を示すイメージ図。

【図８】

実施の形態５におけるデータベース管理装置及びＳＡＤの概略を示すイメージ図。

【図９】

従来のＩＰＳＥＣ機能を搭載したルータを使用したネットワークシステムの概略図。

【図１０】

ＩＰＳＥＣ機能を搭載したネットワーク接続装置間での接続手順を表した図。

【図１１】

従来技術におけるＳＰＤ（Security Policy Database）の一例。

【図１２】

従来技術におけるＳＡＤ（Security Association Database)の一例。

【図１３】

送信側ネットワーク接続装置におけるＩＰＳＥＣ処理のフローチャート。

【図１４】

受信側ネットワーク接続装置におけるＩＰＳＥＣ処理のフローチャート。

【図１５】

時間軸に対応するＳＡの状況を説明するイメージ図。

【符号の説明】

１０１－データベース管理装置

１０２－セキュリティアソシエーションデータベース

１０３－ＳＡＤシステム

１０４－ＳＡＤ制御手段

１０５－関連情報追加手段

１０６－関連情報検索手段

１１１、１３１－ＳＡ

１１２、１３２－送信ホストアドレス

１１３、１３３－受信ホストアドレス

１１４、１３４－プロトコル

１１５、１３５－ＳＰＩ

１１６、１３６－登録時刻

１１７、１３７－有効期間

１１８、１３８－更新待ち時間

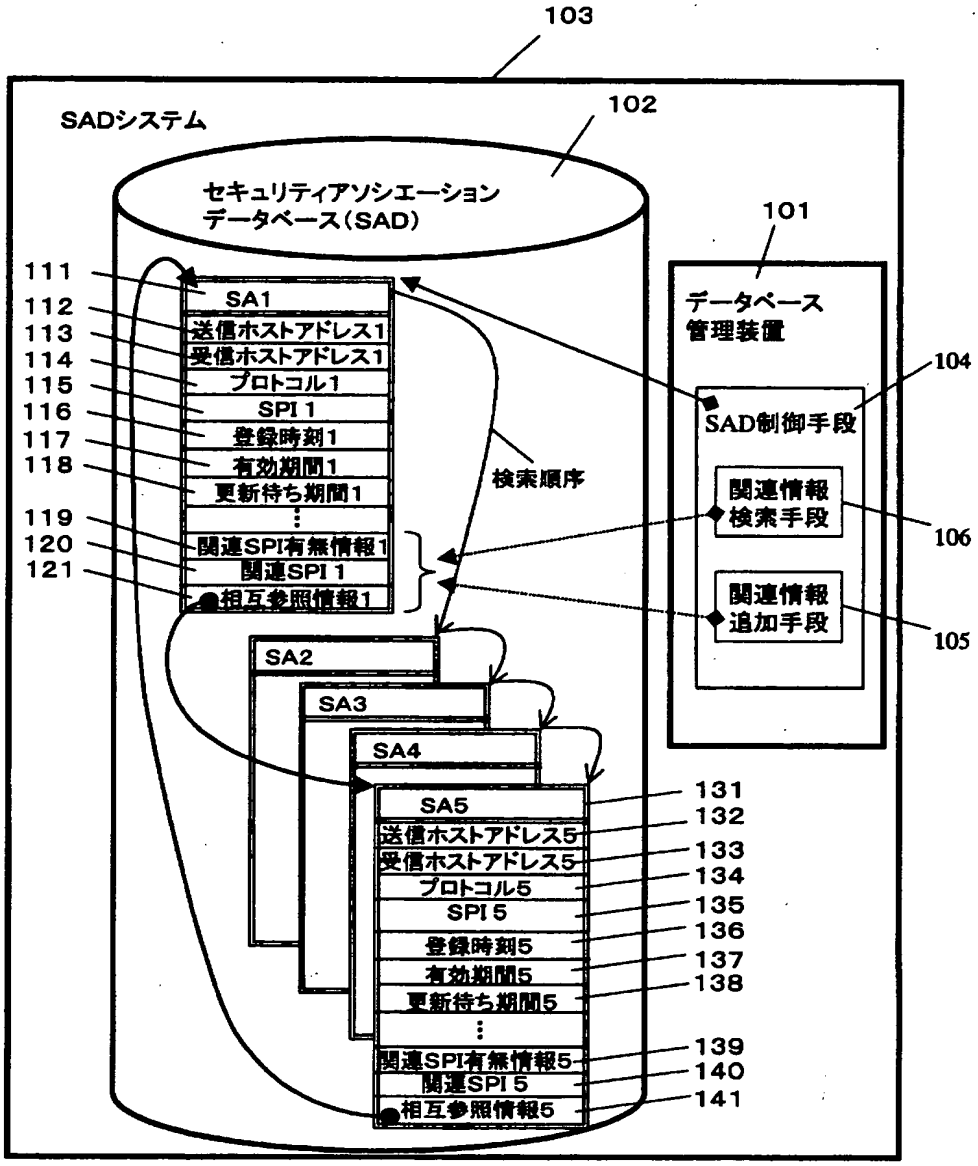
１１９、１３９－関連ＳＰＩ有無情報

１２０、１４０－関連ＳＰＩ

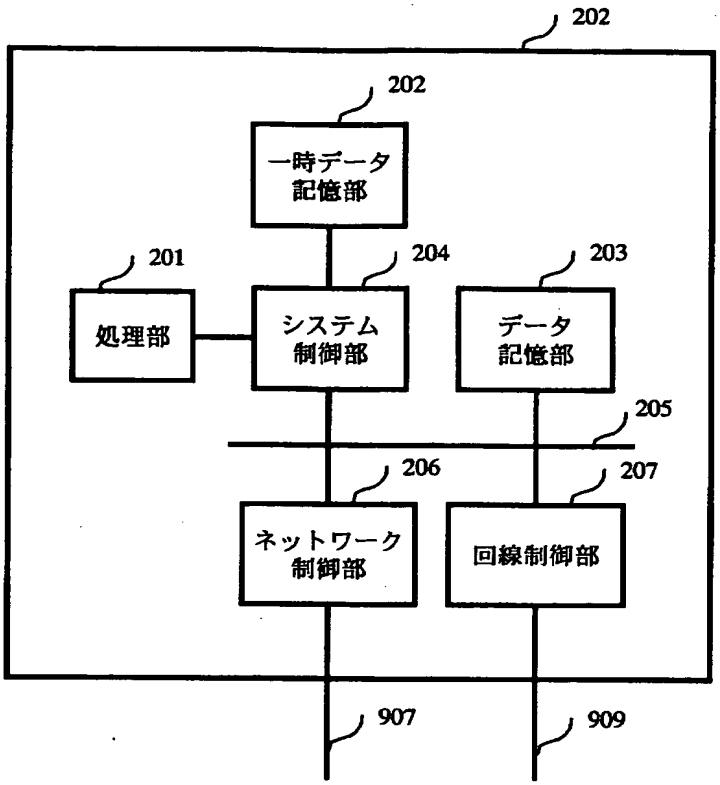
１２１、１４１－相互参照情報

【書類名】　　図面

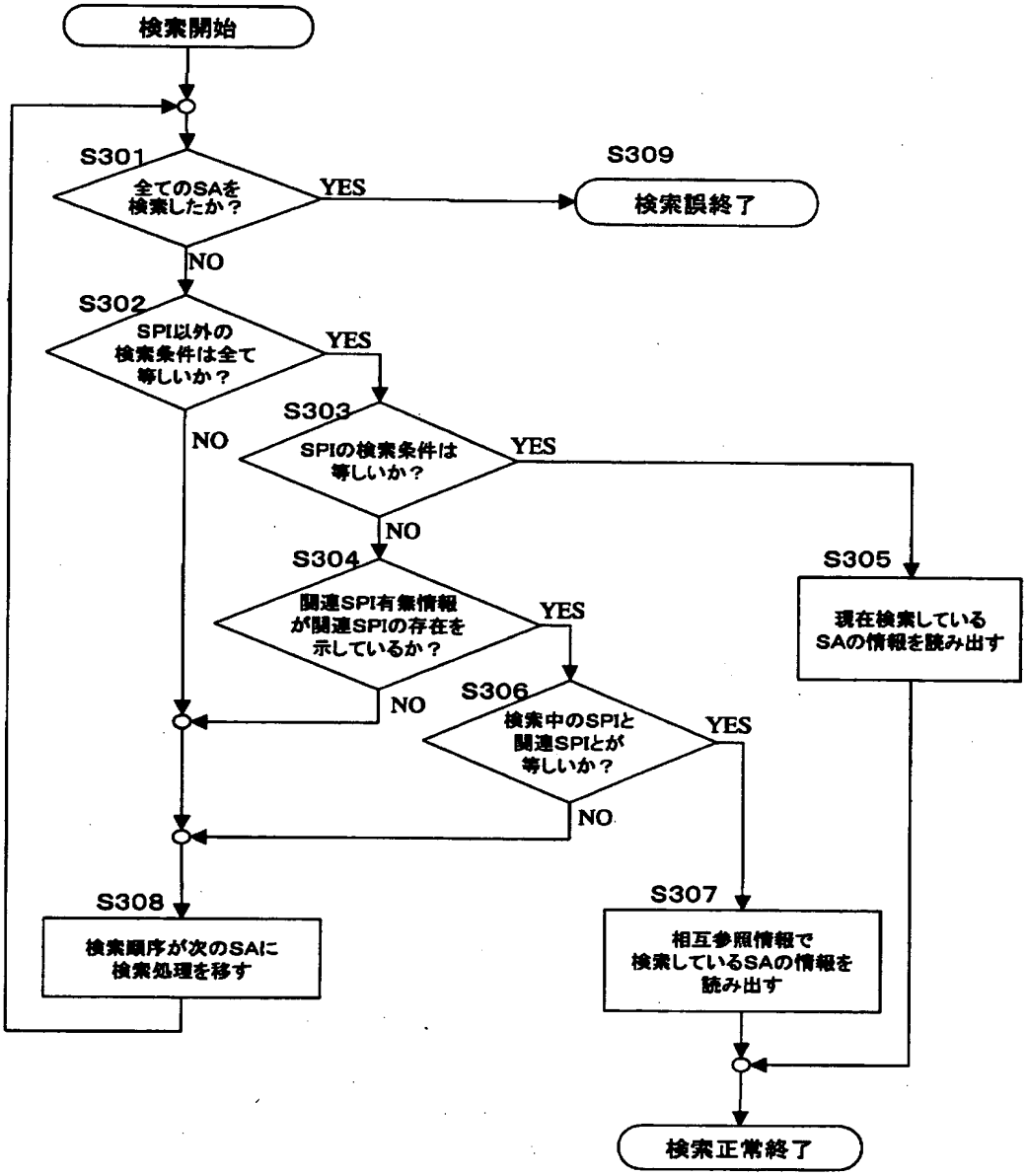
【図１】


103
SADシステム
102
セキュリティアソシエーション
データベース(SAD)
101
データベース
管理装置
104
SAD制御手段
関連情報
検索手段
106
関連情報
追加手段
105
検索順序
111
112
113
114
115
116
117
118
119
120
121
SA1
送信ホストアドレス1
受信ホストアドレス1
プロトコル1
SPI 1
登録時刻1
有効期間1
更新待ち期間1
関連SPI有無情報1
関連SPI 1
相互参照情報1
SA2
SA3
SA4
SA5
送信ホストアドレス5
受信ホストアドレス5
プロトコル5
SPI 5
登録時刻5
有効期間5
更新待ち期間5
関連SPI有無情報5
関連SPI 5
相互参照情報5
131
132
133
134
135
136
137
138
139
140
141

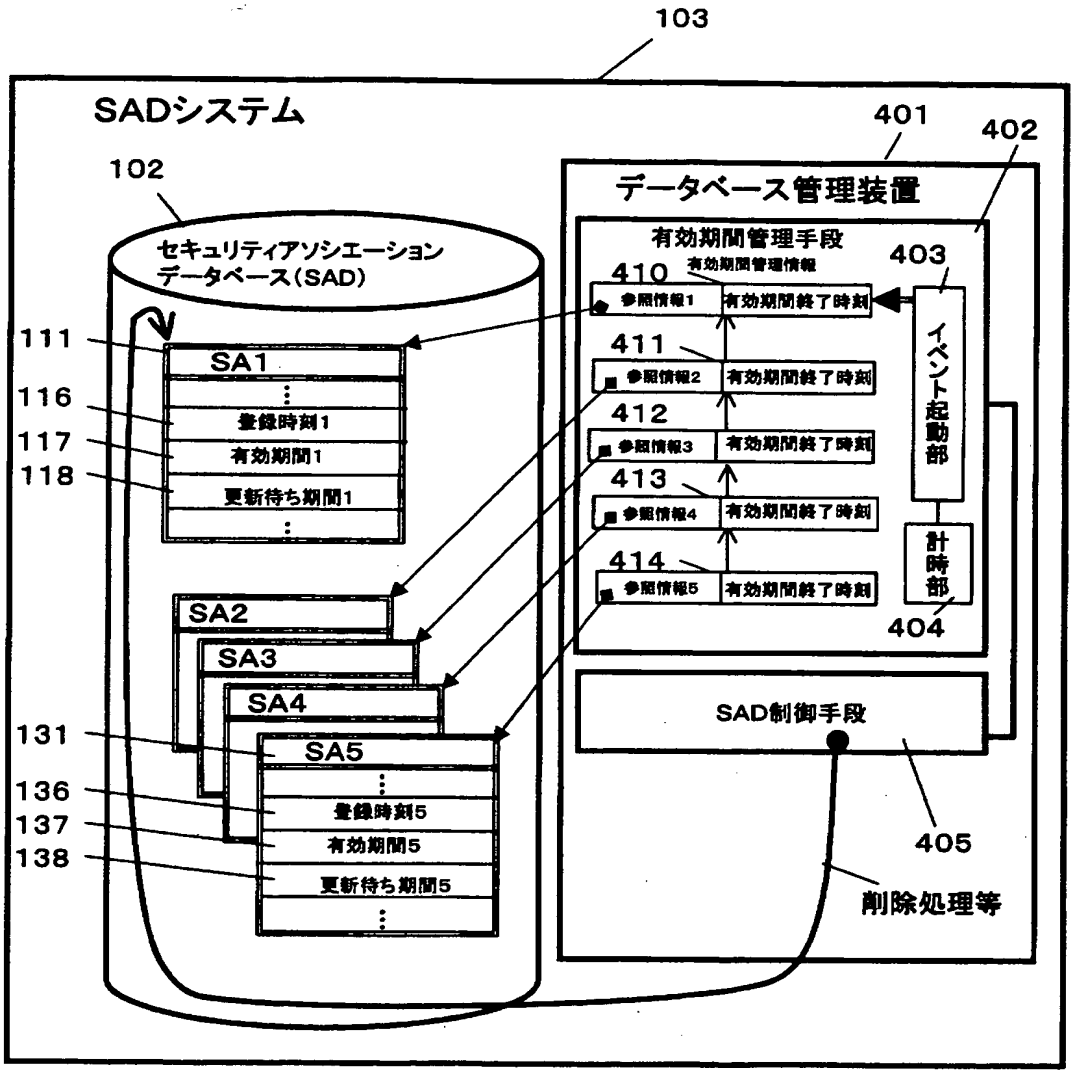
【図２】


202
202
一時データ
記憶部
201
204
203
処理部
システム
制御部
データ
記憶部
205
206
207
ネットワーク
制御部
回線制御部
907
909

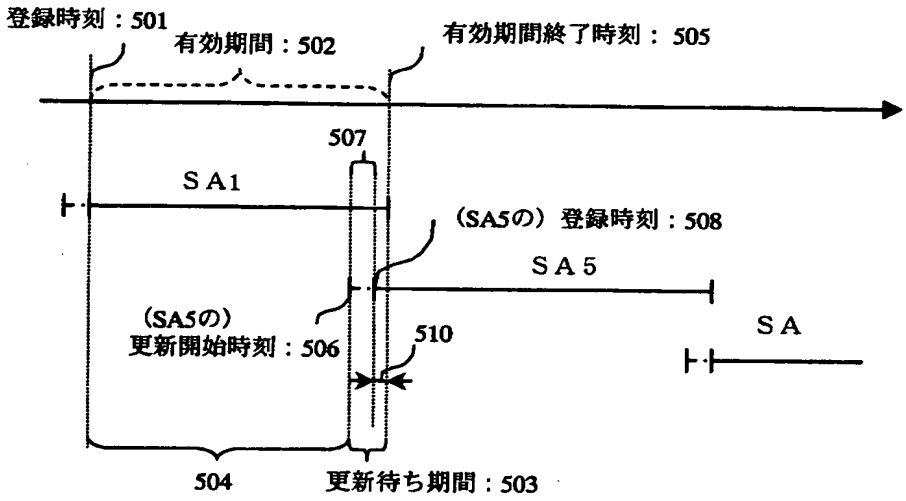
【図３】


検索開始
S301
全てのSAを検索したか？
YES
S309
検索誤終了
NO
S302
SPI以外の検索条件は全て等しいか？
YES
NO
S303
SPIの検索条件は等しいか？
YES
NO
S304
関連SPI有無情報が関連SPIの存在を示しているか？
YES
NO
S305
現在検索しているSAの情報を読み出す
S306
検索中のSPIと関連SPIとが等しいか？
YES
NO
S307
相互参照情報で検索しているSAの情報を読み出す
S308
検索順序が次のSAに検索処理を移す
検索正常終了

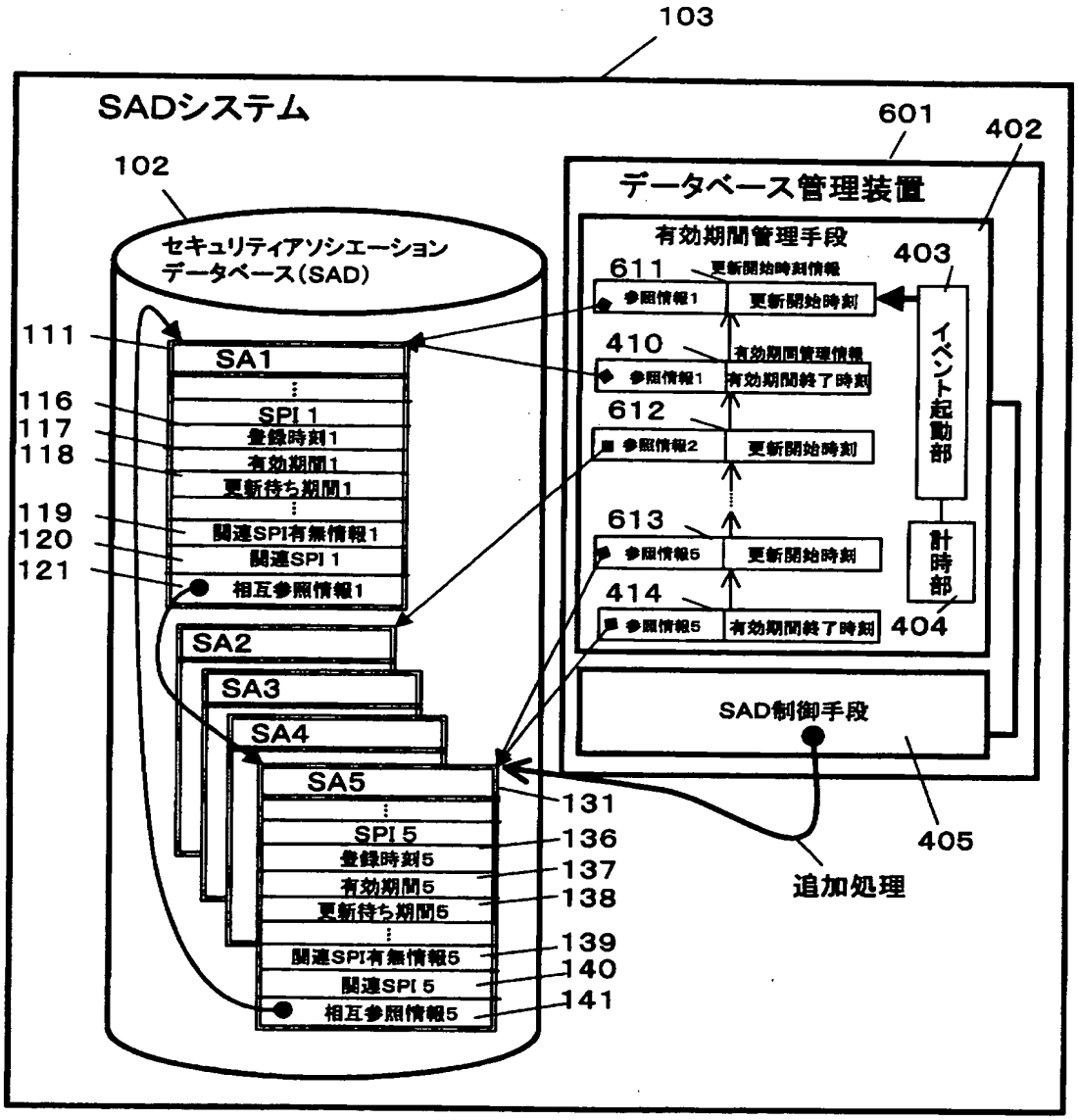
【図４】


103
SADシステム
401
402
102
データベース管理装置
有効期間管理手段
403
セキュリティアソシエーション
データベース(SAD)
410
有効期間管理情報
参照情報1
有効期間終了時刻
111
SA1
411
参照情報2
有効期間終了時刻
116
登録時刻1
412
参照情報3
有効期間終了時刻
117
有効期間1
413
参照情報4
有効期間終了時刻
118
更新待ち期間1
イベント起動部
414
参照情報5
有効期間終了時刻
計時部
404
SA2
SA3
SA4
131
SA5
SAD制御手段
136
登録時刻5
405
137
有効期間5
138
更新待ち期間5
削除処理等

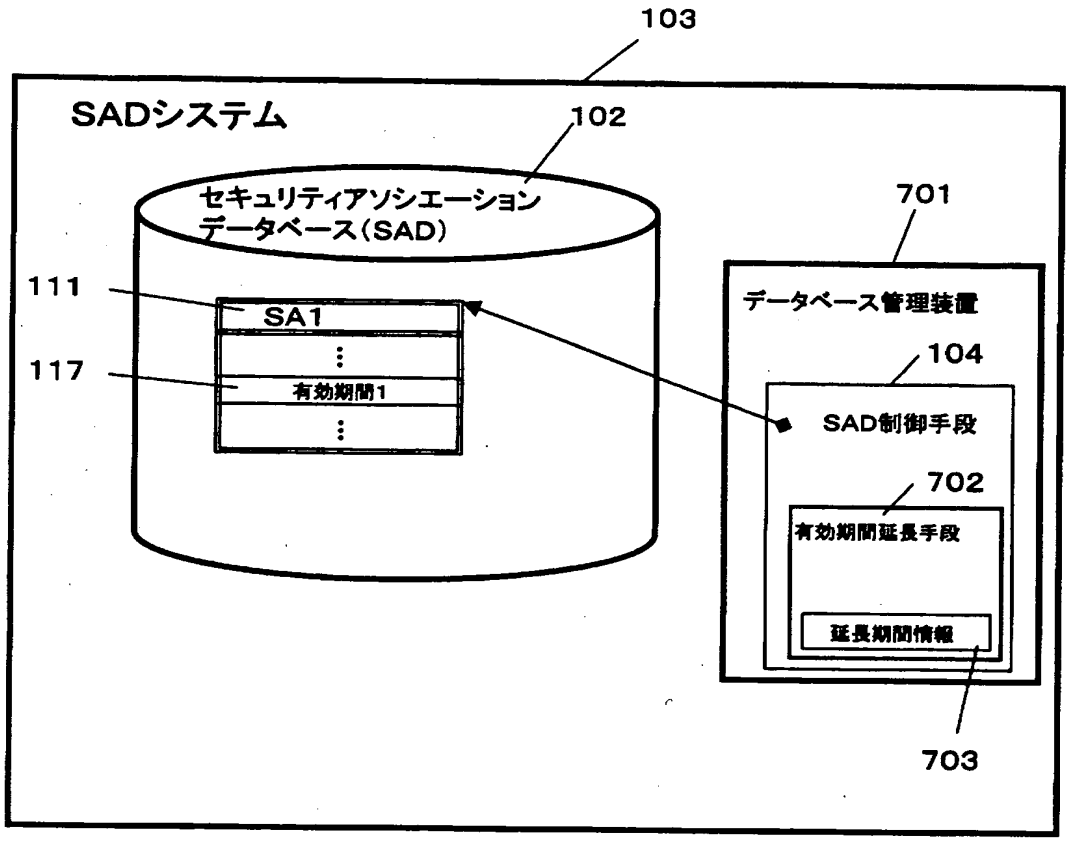
【図５】


登録時刻：501
有効期間：502
有効期間終了時刻：505
507
ＳＡ1
（SA5の）登録時刻：508
ＳＡ５
（SA5の）
更新開始時刻：506
510
ＳＡ
504
更新待ち期間：503

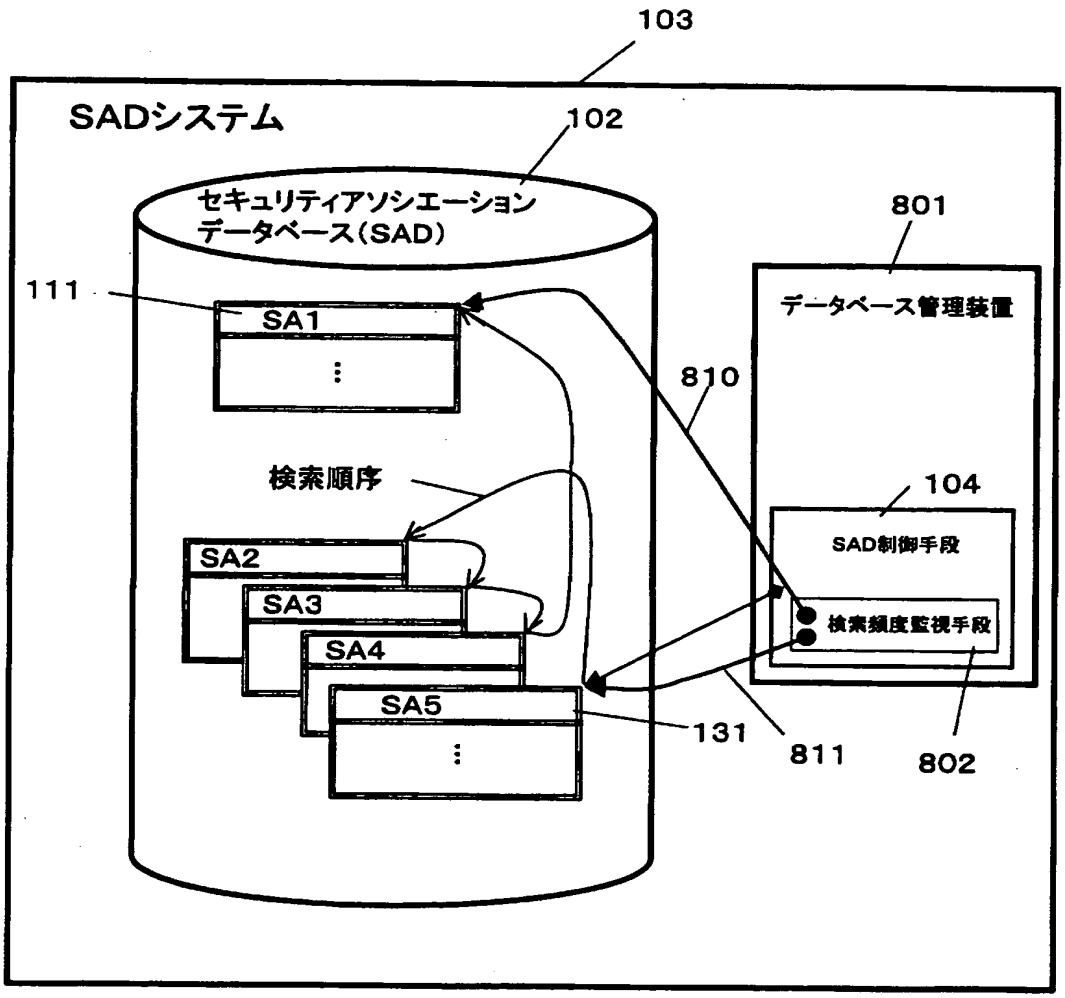
【図６】


103
SADシステム
601
402
102
データベース管理装置
有効期間管理手段
403
セキュリティアソシエーション
データベース(SAD)
611
更新開始時刻情報
参照情報1
更新開始時刻
410
有効期間管理情報
参照情報1
有効期間終了時刻
612
参照情報2
更新開始時刻
613
参照情報5
更新開始時刻
414
参照情報5
有効期間終了時刻
イベント起動部
計時部
404
111
SA1
SPI 1
116
117
118
登録時刻1
有効期間1
更新待ち期間1
119
120
121
関連SPI有無情報1
関連SPI 1
相互参照情報1
SA2
SA3
SA4
SA5
SAD制御手段
131
SPI 5
136
登録時刻5
137
有効期間5
138
更新待ち期間5
139
関連SPI有無情報5
140
関連SPI 5
141
相互参照情報5
405
追加処理

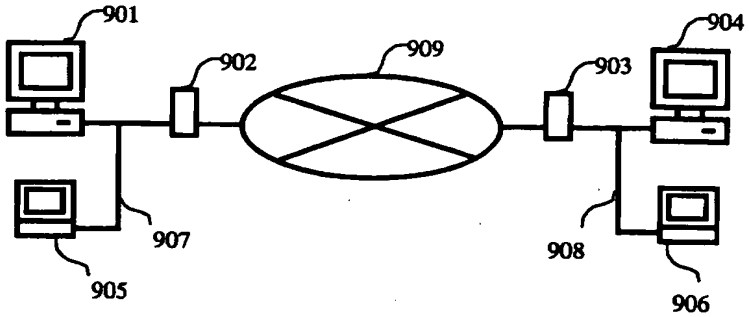
【図７】


103
SADシステム
102
セキュリティアソシエーション
データベース(SAD)
111
SA1
117
有効期間1
701
データベース管理装置
104
SAD制御手段
702
有効期間延長手段
延長期間情報
703

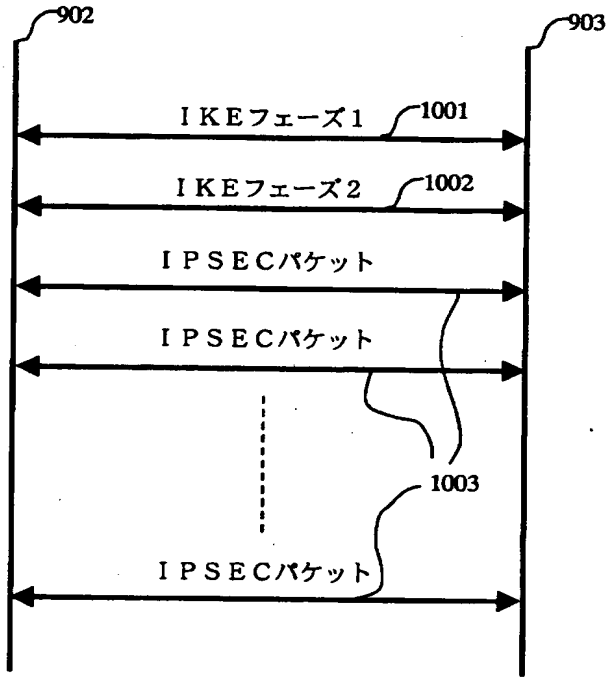
【図８】


103
SADシステム
102
セキュリティアソシエーション
データベース(SAD)
801
111
SA1
データベース管理装置
810
検索順序
104
SAD制御手段
SA2
SA3
検索頻度監視手段
SA4
SA5
131
811
802

【図９】


901
902
909
903
904
907
908
905
906

【図１０】

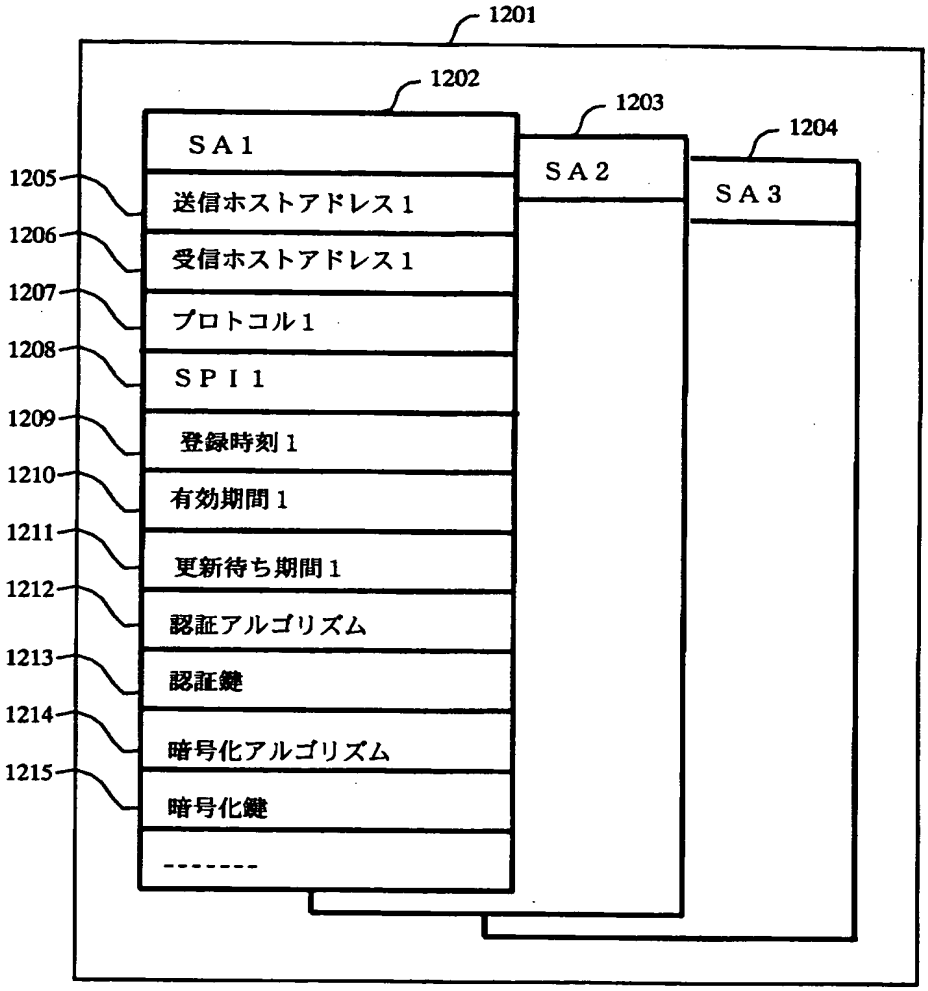


【図１１】

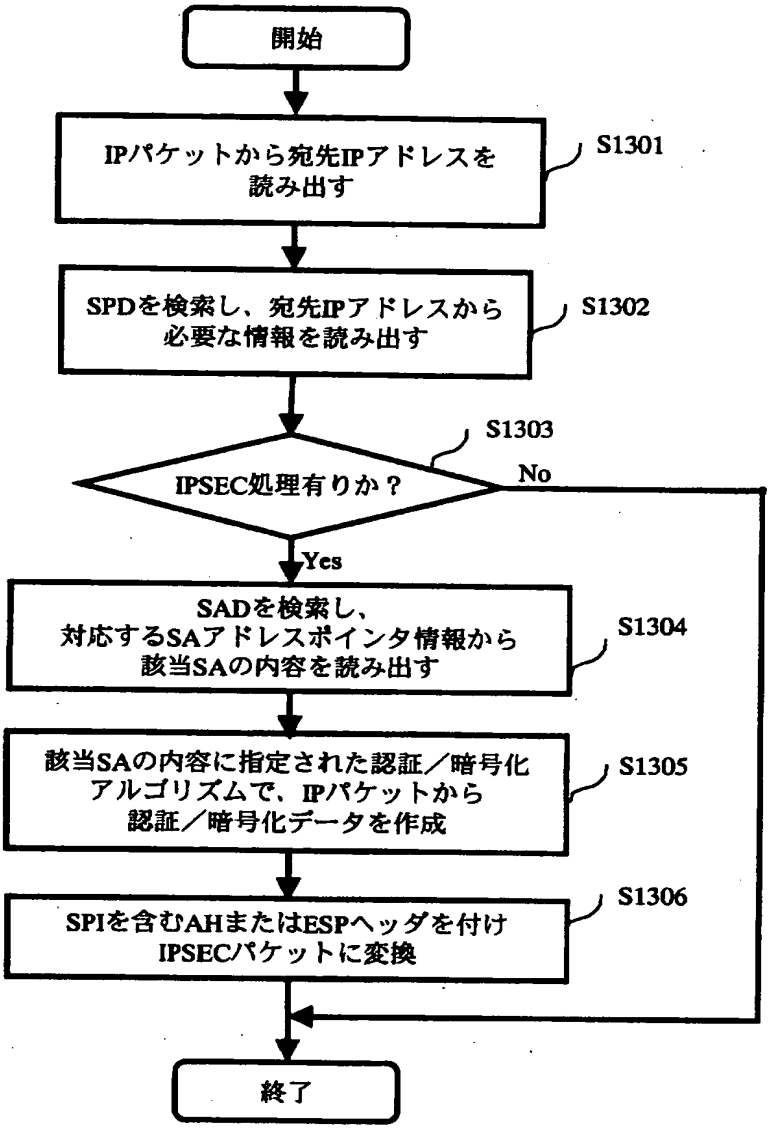
1101

1102	1105	1103	1104
ＩＰＡ－１	ＩＰＳＥＣ－ＩＰＡ－１	有	ＳＡ１
ＩＰＡ－２	ＩＰＳＥＣ－ＩＰＡ－２	無	—
ＩＰＡ－３	ＩＰＳＥＣ－ＩＰＡ－３	有	ＳＡ３
-------	-------	------	-------
ＩＰＡ－Ｌ	ＩＰＳＥＣ－ＩＰＡ－Ｌ	有	ＳＡＭ

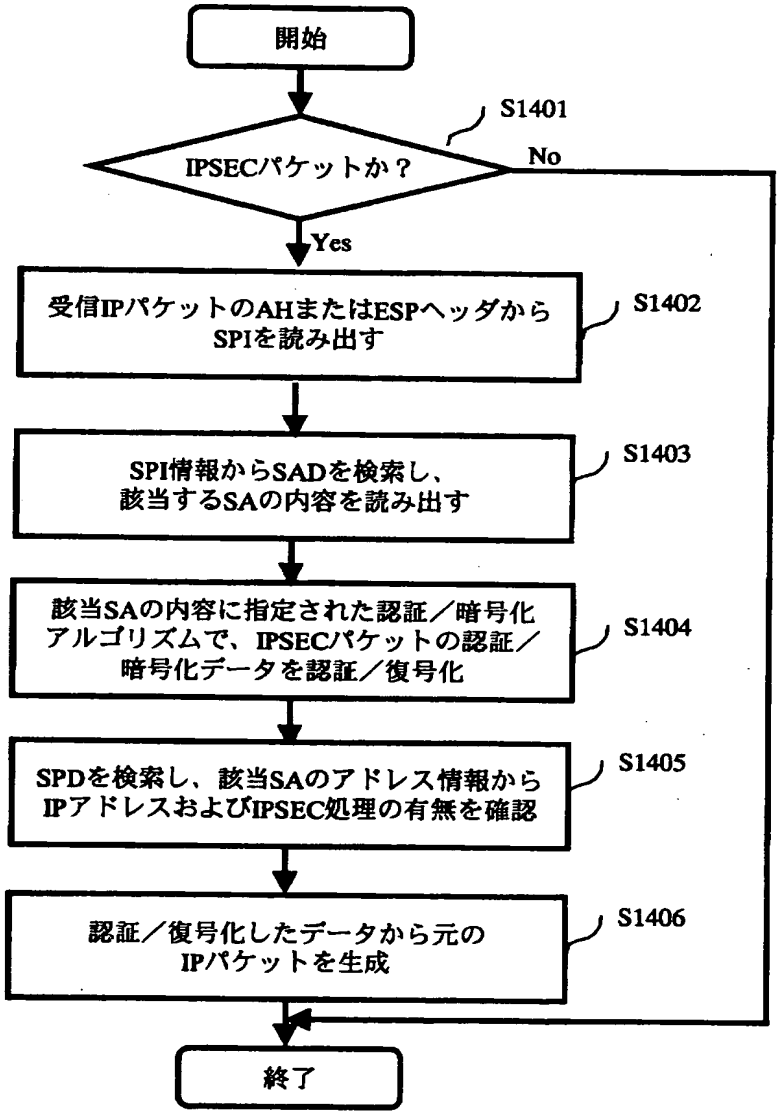
【図１２】


1201
1202
1203
1204
ＳＡ１
ＳＡ２
ＳＡ３
1205
送信ホストアドレス１
1206
受信ホストアドレス１
1207
プロトコル１
1208
ＳＰＩ１
1209
登録時刻１
1210
有効期間１
1211
更新待ち期間１
1212
認証アルゴリズム
1213
認証鍵
1214
暗号化アルゴリズム
1215
暗号化鍵

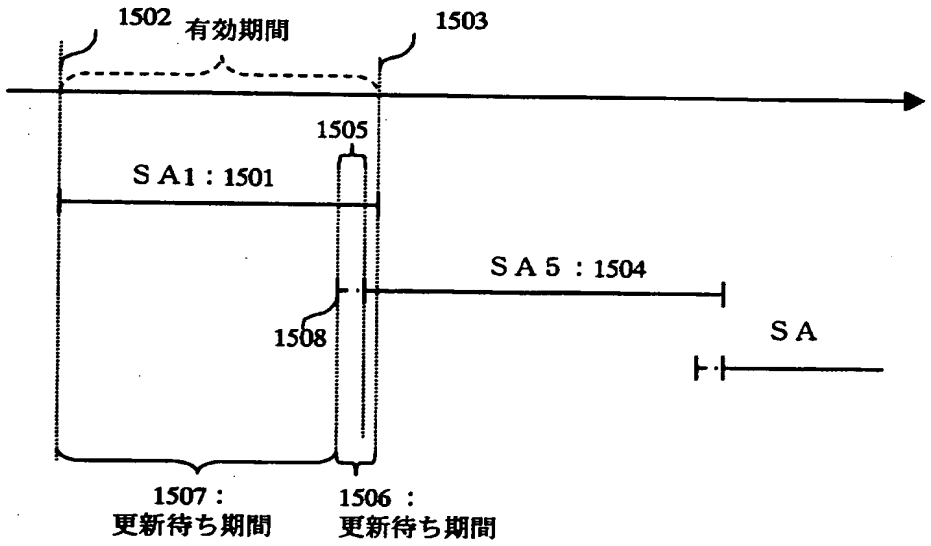
【図１３】


開始
IPパケットから宛先IPアドレスを読み出す
S1301
SPDを検索し、宛先IPアドレスから必要な情報を読み出す
S1302
S1303
IPSEC処理有りか？
No
Yes
SADを検索し、対応するSAアドレスポインタ情報から該当SAの内容を読み出す
S1304
該当SAの内容に指定された認証／暗号化アルゴリズムで、IPパケットから認証／暗号化データを作成
S1305
SPIを含むAHまたはESPヘッダを付けIPSECパケットに変換
S1306
終了

【図１４】


開始
S1401
IPSECパケットか？
No
Yes
受信IPパケットのAHまたはESPヘッダから
SPIを読み出す
S1402
SPI情報からSADを検索し、
該当するSAの内容を読み出す
S1403
該当SAの内容に指定された認証／暗号化
アルゴリズムで、IPSECパケットの認証／
暗号化データを認証／復号化
S1404
SPDを検索し、該当SAのアドレス情報から
IPアドレスおよびIPSEC処理の有無を確認
S1405
認証／復号化したデータから元の
IPパケットを生成
S1406
終了

【図１５】


1502
有効期間
1503
1505
ＳＡ1：1501
ＳＡ５：1504
1508
ＳＡ
1507：
更新待ち期間
1506：
更新待ち期間

【書類名】　　要約書

【要約】

【課題】　データベース内の検索対象となるデータを短時間に検索すると共に、有効期間の終了するデータと当該データの後継データとの切換をスムーズに行うデータベース管理装置、管理方法及びその記録媒体を提供する。

【解決手段】　有効期間が終了する所定のデータと、当該所定のデータに対応する後継データとの両方又はどちらか一方に上記データを相互に関連付けた関連情報を追加する関連情報追加手段を具備するデータベース管理装置、管理方法及び記録媒体を提供する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社